Cybersecurity and Incident Response

presented by the
Northeastern Indiana Chapter

08/26/15

A Workshop for the Incident Response Team!

by

Dan Hadaway, CRISC CISA CISM

infotex

Building Your
Incident Response Program

Dan Hadaway CRISC CISA CISM
Managing Partner
infotex

infotex

With Extra Scenes!

Cybersecurity
Assessment Tool!

FFIEC Cybersecurity Assessment Tool

Extra Scenes!

June 30th, 2015

www.ffiec.gov/cyberassessmenttool.htm

FFIEC Cybersecurity Assessment Tool

Process Flow for Institutions:

Step 1: **Read Overview for Chief Executive Officers and Boards of Directors** to gain insights on the benefits to institutions of using the Assessment, the roles of the CEO and Board of Directors, a high-level explanation of the Assessment, and how to support implementation of the Assessment.

Step 2: **Read the User's Guide** to understand all of the different aspects of the Assessment, how the inherent risk profile and cybersecurity maturity relate, and the process for conducting the Assessment.

Step 3: **Complete Part 1: Inherent Risk Profile of the Cybersecurity Assessment Tool** to understand how each activity, service, and product contribute to the institution's inherent risk and determine the institution's overall inherent risk profile and whether a specific category poses additional risk.

Step 4: **Complete Part 2: Cybersecurity Maturity of the Cybersecurity Assessment Tool** to determine the institution's cybersecurity maturity levels across each of the five domains.

Step 5: **Interpret and Analyze Assessment Results** to understand whether the institution's inherent risk profile is appropriate in relation to its cybersecurity maturity and whether specific areas are not aligned. If management determines that the institution's maturity levels are not appropriate in relation to the inherent risk profile, management should consider reducing inherent risk or developing a strategy to improve the maturity levels.

Refer to the User's Guide for additional explanation of Steps 3, 4, and 5.

In addition to the "Overview for Chief Executive Officers and Boards of Directors", the FFIEC has released the following documents to assist institutions with the Assessment.

- Appendix A: Mapping Baseline Statements to FFIEC IT Handbook
- Appendix B: Mapping to NIST Cybersecurity Framework
- Appendix C: Glossary

Paperwork Reduction Act
OMB Control No. 1557-0328
Expiration Date: December 31, 2015
A Federal agency may not conduct or sponsor, and an organization (or person) is not required to respond to, a collection of information unless it displays a currently valid OMB control number

What I have heard about the CAT

- It's a voluntary tool responding to requests for a way to understand our "cyber preparedness" due to increased volume of cyber-attacks.
- Financial Institutions are not Required to Use It
- It's not an examination program

FFIEC Cybersecurity Assessment Tool

What I have heard about the CAT

- The FFIEC Intends to:
  - Update the IT Examination Work Program that Examiners Use
  - Update the Information Security Handbook (circa 2006)
  - Launch a Cybersecurity Outreach Program

FFIEC Cybersecurity Assessment Tool

What I will say about the CAT

- Slow down, keep your wallets in your pocket, take a deep breath
- Reflects Incident Response as the intersection of Awareness, Risk Management, and Business Continuity. It integrates the NIST Cybersecurity Framework with the Capability Maturity Model
  - Five Levels of "Maturity" instead of a Yes/No approach to "closed."

FFIEC Cybersecurity Assessment Tool

Capability Maturity Model

- *Initial* (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.
- *Repeatable* - the process is at least documented sufficiently such that repeating the same steps may be attempted.
- *Defined* - the process is defined/confirmed as a standard business processes.
- *Managed* - the process is quantitatively managed in accordance with agreed-upon metrics. Tested.
- *Optimizing* - process management includes deliberate process improvement. Repeatedly passing tests.

CAT Maturity Levels

Baseline	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
Evolving	Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.
Intermediate	Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.
Advanced	Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
Innovative	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.

FFIEC Cybersecurity Assessment Tool

Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Frameworks
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Frameworks
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

How Weôll Do It!

Å First weôll learn each otherôs name!

infotex

Weôll Play a Trivia Game

Dan will ask a question.

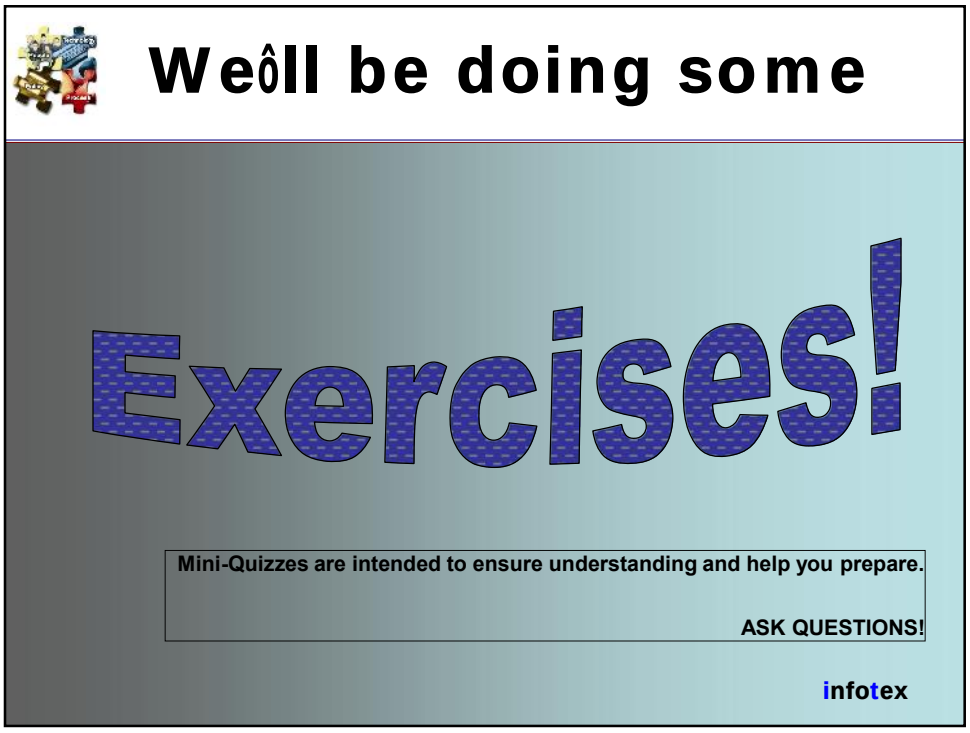
A. Yell out the answer!

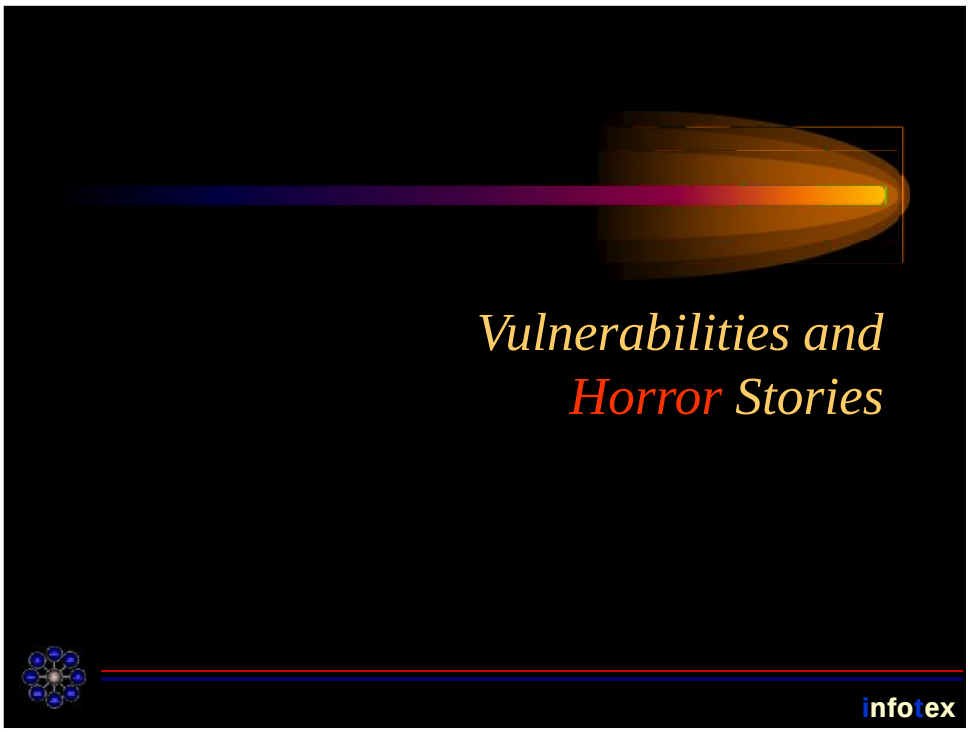
B. Help Chad guess who got the right answer first!

C. Figure thereôs a reason the question is being asked!

D. All of the above!

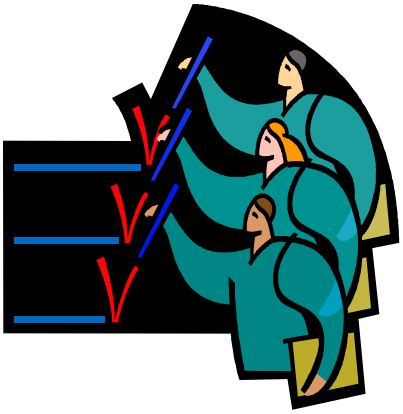
infotex


We'll be doing some
Exercises!
Mini-Quizzes are intended to ensure understanding and help you prepare.
ASK QUESTIONS!
infotex


Vulnerabilities and
Horror Stories
infotex

Thereôll be homework . . .

- Electronic copies of pertinent policies, procedures, and tools will be available on our ñworkshop portal.ò



infotex

Incident Response Program

- **Let's see the directory structure!**

infotex

Simplify IT

- Dan will try to simplify it.

infotex

Simplify IT

- Three primary tools of this workshop!
  - Workbook
  - Dan's PowerPoint
  - Portal

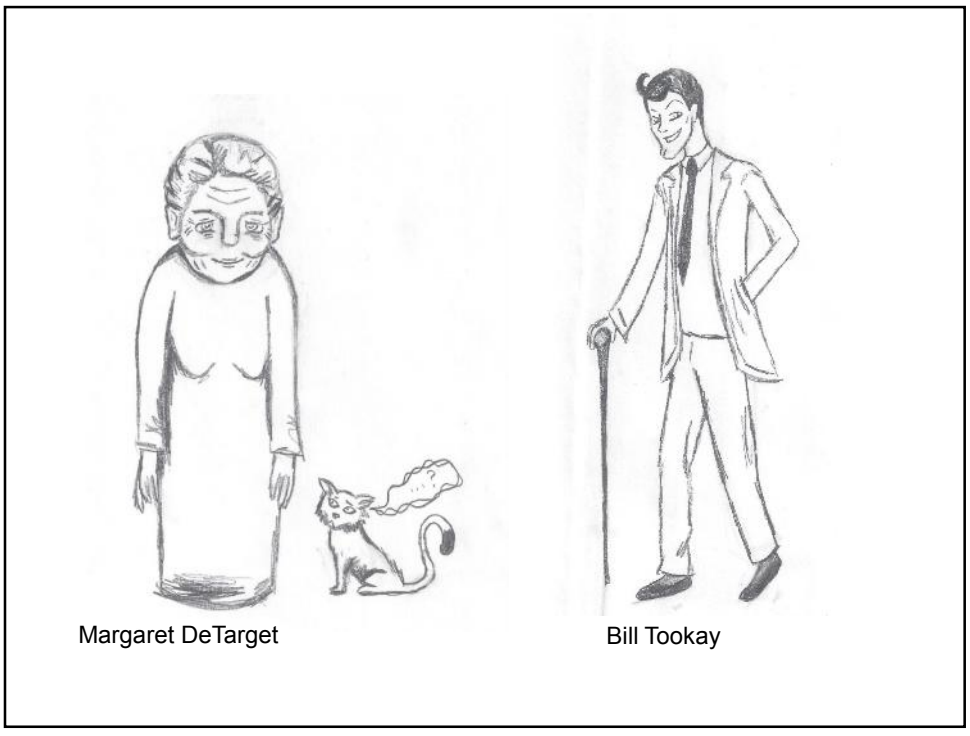
infotex

Whoôs here?

- Name
- Title (or role)
- Your Bank
- Your Town
- Size of your Bank
- Are you primarily technical or non-technical?

infotex

Whoôs Missing?
IZO
Americas Next Top Model
HACKER
Mark Etting
Joe 17.0
Percí Nell
Joan DPartmen
Hacker Guy


Margaret DeTarget
Bill Tookay

Our Credentials

- Information Security
  - CRISC (a risk management certification)
  - CISAs, CISMs, CISSPs
  - Experienced first incident in 1989
  - Conducted first risk assessment in 1989
  - Updating our "process" annually
- Not . . . BSA, OFAC, FACTA,
- Not Red Flags, CIP, KNC

infotex

Our Credentials

- Worked with banks since 2000.
  - (July 24th 2015, our Anniversary!)
- Have a 80:20 ratio banks to credit unions.
- Naturally struggle with the customer/member dichotomy, and discover awkward expressions when I try to say "institution."

infotex

This Workshop

- First presented at the CBAI in 2004.
- Presented (almost) annually at the IBA since about 2007.
- This slidedeck is based on a workshop delivered on June 4th.
- Is pre-CAT.

infotex

Where are we in the process?

- We're slowing down and thinking this through.
- We are going to integrate a maturity level color coding scheme into our boilerplates.
- This workshop will talk a LOT about the CAT, but we've got conferences and workshops to go to of our own!

infotex

Disclosure

We are an MSSP.

- In fact, we are the preferred service provider for the Indiana Bankers Association.
- There are other legitimate players in the industry as well. We have listed them in the back of our manual.

IBA INDIANA BANKERS™ ASSOCIATION

infotex

A Note About Nomenclature

- Everybody has their own terminology.
- What is important is the concept.
- Be on the lookout for terminology that your examiners are currently using.

infotex

Nomenclature

- We assume the ISO is the coordinator of the Incident Response Process, but this isnôt always the case.
- We use CIRT (Computer Incident Response Team) only when we didnôt find it to change it to IRT (Incident Response Team) reflecting that some incidents are not computer-related.

infotex

Regarding Guidance

- FFIEC Guidance was all over the place on Incident Response.
- Iôll be teaching from four primary documents:
  - FDICôs FIL 2005-27
  - NIST SP 800-61
  - NIST CyberSecurity Framework
  - FFIEC CyberSecurity Assessment Tool

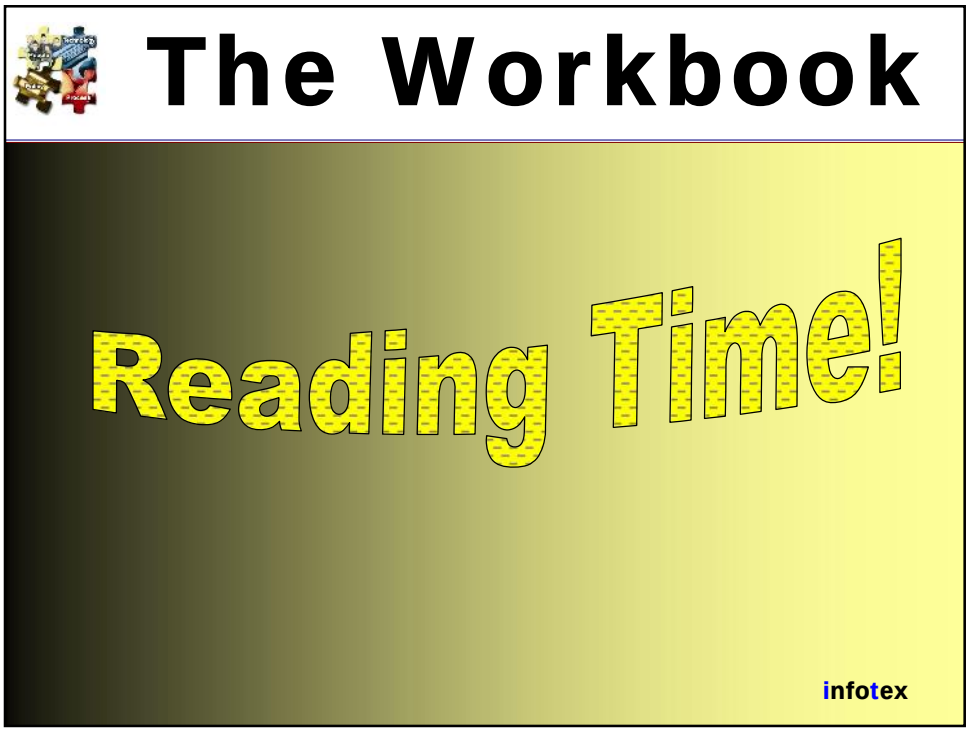
infotex

Regarding Guidance

- OCC: Bulletin 2005-13
- Fed: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
  - (In federal register.)
  - Copy on portal.
  - Or you can refer to FFIEC.gov Appendix B part 364

infotex

infotex



Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Frameworks
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

Today's Agenda

- Incident Response Fundamentals:
  - Risks of Incident Response
  - Goals of Incident Response
  - Compliance Frameworks

Today's Agenda

- But first:
  - Risks of Incident Response
  - Goals of Incident Response
  - Compliance Frameworks

Incident Response

They were:
- Transparent
- Quick to Respond
- Truthful

Their response left us with the belief they valued the health of their customers.

Followed a Prioritized Process:

- They **contain**ed the incident.
- The **eradicate**d it's cause.
- After **recover**y, their
- Transparent **follow-up** made sure it could never happen again.

Incident Response

Time for a couple of movies!

Post-Mortem Review (March 2014)
https://www.youtube.com/watch?v=M5tl4Yf92Nk

January 10th, 2014
https://www.youtube.com/watch?v=w1o52wMzjFw

infotex

Incident Response

TARGET

Malware installed to capture credit card numbers stored those numbers on a Target server.

FireEye (an MSSP) saw the ex-filtration and alerted Target.

Nothing happened.

(There was no triage process.)

What happened?

Malware installed to capture credit card numbers stored those numbers on a Target server (11/27/13)

FireEye (an MSSP) did not notice the malware ñbehavingò until 11/30/13.

FireEye did not notice the behavior until 11/30/13.

FireEye saw data ex-filtration and alerted Target repeatedly for two weeks.

On 12/15, after law enforcement and a forensics company joined FireEye, Target removed the malware.

Breach Timeline

Target did not notify customers of credit card theft until 20 days after being informed of the breach.

That was 12/19 . . . still in time to execute recovery before Christmas. Credit Card Only.

But the Target had to turn back around and notify of the loss of PII on January 10th.

Making Matters Worse

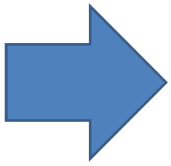
Target had not integrated the non-technical (escalation, triage) with the technical (intrusion detection)

Target chose PCI as their compliance framework, did not understand the value of the data that was breached (or they would have included PII in their original announcement)

While Target had invested in the necessary tools, they did not see them for what they were: awareness tools still only as good as the users using them.

Conclusions

Incident Response



Conclusions

Business Continuity

Risk Management

Awareness

Target had not integrated the non-technical (escalation, triage) with the technical (intrusion detection)

Target chose PCI as their compliance framework, did not understand the value of the data that was breached (or they would have included PII in their original announcement)

While Target had invested in the necessary tools, they did not see them for what they were: awareness tools still only as good as the users using them.

See Incident Response As . . .

Risks of Un-monitored Risk

- Likelihood increases
- Reputation is at risk
- Team Confidence suffers
- Change Management Falters
- Unnecessary Denial of Service (DoS)
- Compliance Deficiencies
- Unauthorized access

infotex

Let's go around the room

- What other risks can you think of?

Today's Agenda

- But first:
  - Risks of Incident Response
  - Goals of Incident Response
  - Compliance Frameworks

Types of Goals

- Pro-active Goals
- Re-active Goals
- Re-active Pro-active Goals
- Incident Priorities

infotex

. . . but first . . .

Simplify IT

- The first priority of any incident
  1. Containment
  2. Everything else comes second.

infotex

Types of Goals

- Pro-active Goals
- Re-active Goals
- Re-active Pro-active Goals
- Incident Priorities

infotex

Pro-active Goals of Incident Response

- Assure integrity of critical information assets.
- Detect intrusion, misuse, and other negative events.

infotex

Pro-active Goals of Incident Response

- Recover systems, data, and services.
- Contain intrusions and negative incidents.
  - See containment as isolation.
  - Can be as simple as putting your device in airplane mode!

infotex

Re-active Goals of Incident Response

- Investigate the source or cause of an incident.
- Facilitate and control communication with internal and external agencies.

infotex

Re-active Goals of Incident Response

- Investigate in a manner that will allow prosecution where appropriate.
- Feed the Suspicious Activity Reporting procedure.

infotex

Re-active Pro-active Goals!

- Allow for trend analysis, on-going risk assessment, and mitigation.
- Educate IRT.
- Heighten Awareness of appropriate team members.
- Update Decision Tree.

infotex

Priorities of an Incident

1. Protect human life and safety.
2. Protect customer information and assure organizational data integrity.

infotex

Priorities of an Incident

3. Maintain the financial institutionôs reputation and control external communication.
4. Prevent damage to systems.
5. Minimize disruption of computing resources.

infotex

Simplify IT

- The first three steps in an incident:
  1. Broadcast Awareness
  2. Inform the Information Security Officer
  3. Assist in the Triage Process

infotex

Today's Agenda

- But first:
  - Risks of Incident Response
  - Goals of Incident Response
  - Compliance Frameworks

Disclosure of Breach

Å Indiana Code 24-4.9

- ï Requires disclosure of breach of data to all persons whose data was breached.
- ï Defines what constitutes a breach.
- ï Defines penalties for non-disclosure.
- ï Exempts Indiana government agencies, judiciary, and legislation.

infotex

Indiana Code 24-4.9

- Definitions
  - Breach of Data Security
    - Unauthorized acquisition (electronic and hard copy)
    - Exempts ñredactedò and ñencryptedò
  - Doing business in Indiana
  - Defines ñPersonal Informationò

infotex

ñBreach of Data Securityò

- A) means:
  - unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person.
  - The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

infotex

ñBreach of Data Securityò

- (b) The term does not include the following:
  - (1) Good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure.
  - (2) Unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key:
    - (A) has not been compromised or disclosed; and
    - (B) is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device.

infotex

ñPersonal Informationò

- **IC 24-4.9-2-10**

(1) a Social Security number that is not encrypted or redacted; or

(2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:

(A) A driver's license number.

(B) A state identification card number.

(C) A credit card number.

(D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

infotex

Disclosure of Breach

- Indiana Code 24-4.9
  - Requires disclosure of breach of data to all persons whose data was breached.
  - Defines what constitutes a breach.
  - Defines penalties for non-disclosure
  - Exempts Indiana government agencies, judiciary, and legislation.

infotex

Indiana Code 24-4.9

- Definitions
  - Defines ñPersonal Informationò
  - Defines Breach of Data Security
    - Unauthorized acquisition (electronic and hard copy)
    - Exempts ñredactedò and ñencryptedò

infotex

ñPersonal Informationò

Å **IC 24-4.9-2-10**

(1) a Social Security number that is not encrypted or redacted; or

(2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:

(A) A driver's license number.

(B) A state identification card number.

(C) A credit card number.

(D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

infotex

Definition of Redaction

Å **IC 24-4.9-2-11**

Redacted data or personal information

Sec. 11. (a) Data are redacted for purposes of this article if the data have been altered or truncated so that not more than the last four (4) digits of:

(1) a driver's license number;

(2) a state identification number; or

(3) an account number;

is accessible as part of personal information.

(b) For purposes of this article, personal information is "redacted" if the personal information has been altered or truncated so that not more than five (5) digits of a Social Security number are accessible as part of personal information.

infotex

Penalties for Nondisclosure

- $150,000 per ñdeceptive act.ò
- Plus Attorney Generalôs costs in investigating the matter.
- Plus court costs.

infotex

Because there's good news!

IC 24-4.9 defers to federal regs

- The process that should be followed by Indiana law does not pre-empt the process required by the FFIEC.
- The FFIEC requires a specific process, once you have determined that a breach has occurred.

infotex

FIL-27-2005

- A PDF of this letter is on our portal (or can be downloaded from various agency websites).
- Weôll review some of its requirements when we talk about customer notification.

infotex

FIL-27-2005

- Indiana Code 24.9-4 is consistent with FIL-27-2005 except:
  - FIL-27-2005 also includes ñaccount credentialsò in its description of what Indiana Code calls ñpersonal information.ò
  - You do NOT have to notify the Stateôs Attorney General (instead, you notify your examiner).

infotex

Another important distinction!

- FIL-27-2005 gives a bit more wiggle-room in the following guidance on when notification should occur:
  - "and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur."

infotex

Policy Definitions

- Disclosure Incidents (per law)
- Security Incidents
- Negative Incidents

infotex

Policy Definitions

- Disclosure Incidents: Always notify the board in real time.
- Security Incidents: Notify the board in real time if critical, otherwise as a trend report.
- Negative Incidents: Notify the board in real time if critical, otherwise as a trend report.

infotex

Do we need a break?

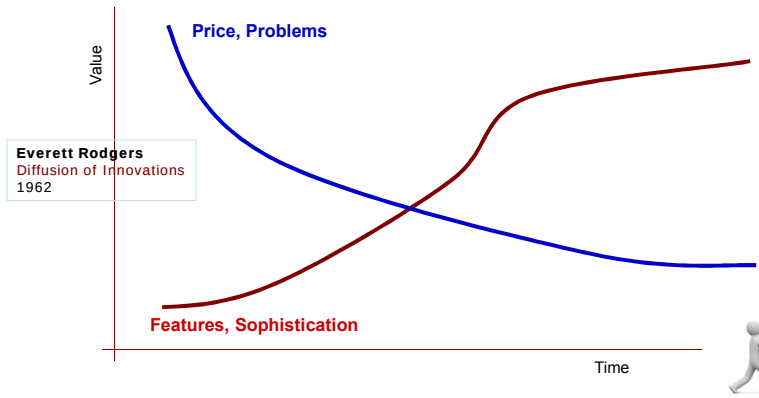
Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Frameworks
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

The Problem

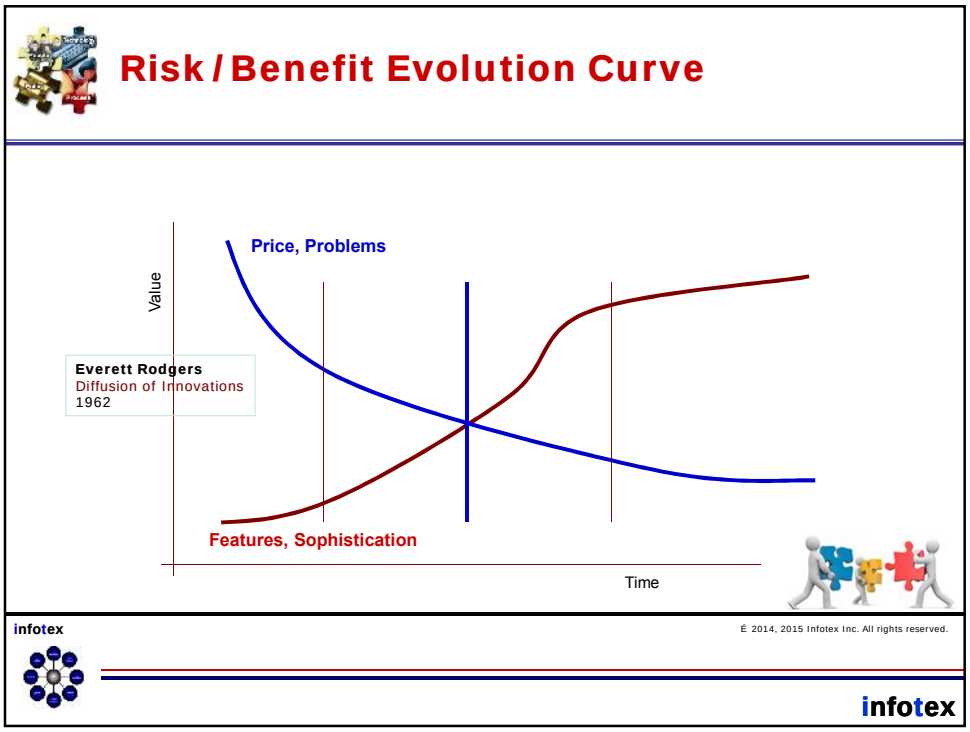
infotex

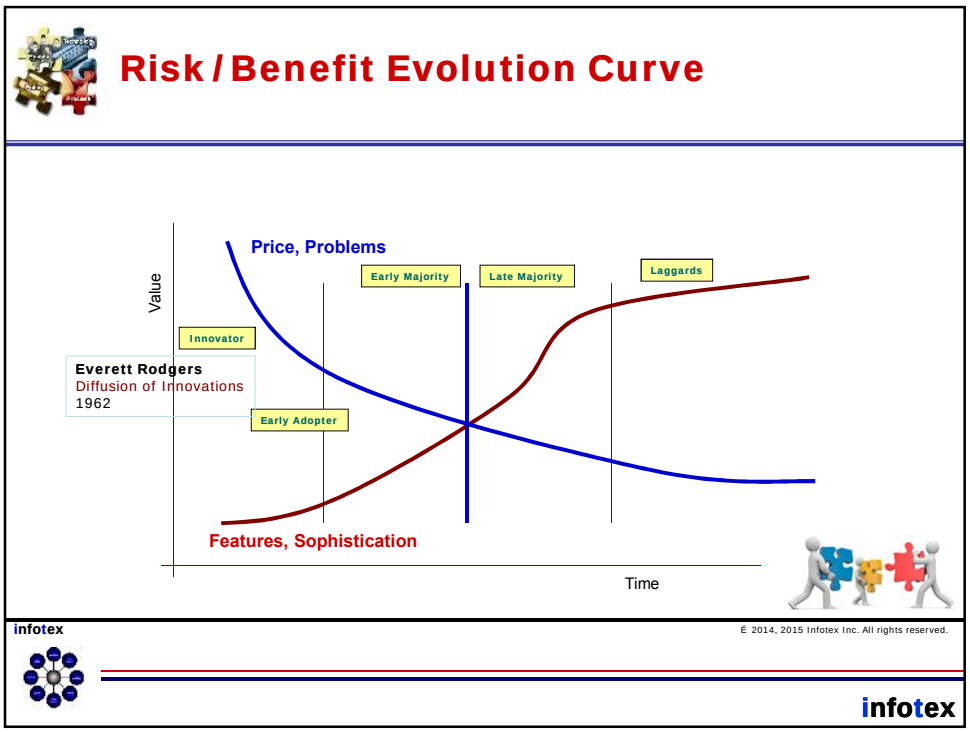
Risk / Benefit Evolution Curve



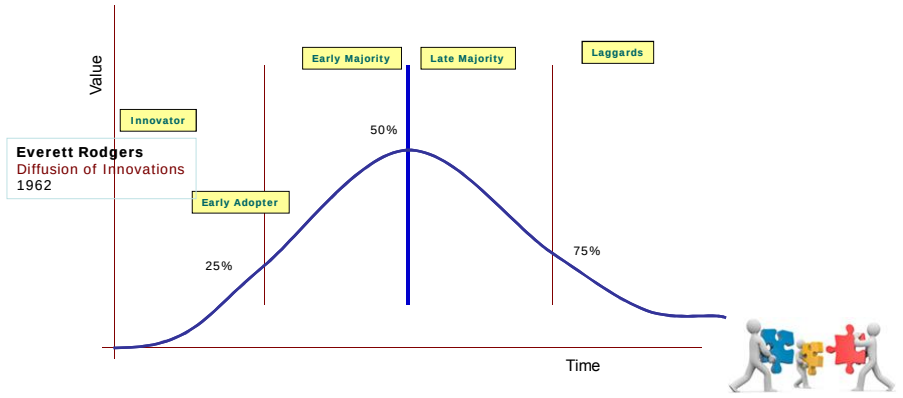
infotex
É 2014, 2015 Infotex Inc. All rights reserved.

infotex


Risk / Benefit Evolution Curve
Price, Problems
Value
Everett Rodgers
Diffusion of Innovations
1962
Features, Sophistication
Time
infotex
© 2014, 2015 Infotex Inc. All rights reserved.
infotex

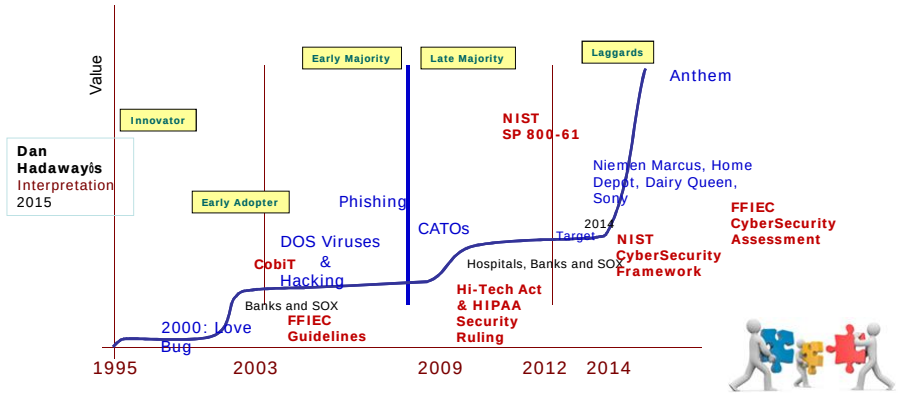

Risk / Benefit Evolution Curve
Price, Problems
Early Majority
Late Majority
Laggards
Value
Innovator
Everett Rodgers
Diffusion of Innovations
1962
Early Adopter
Features, Sophistication
Time
infotex
© 2014, 2015 Infotex Inc. All rights reserved.
infotex

Typical Technology Adoption



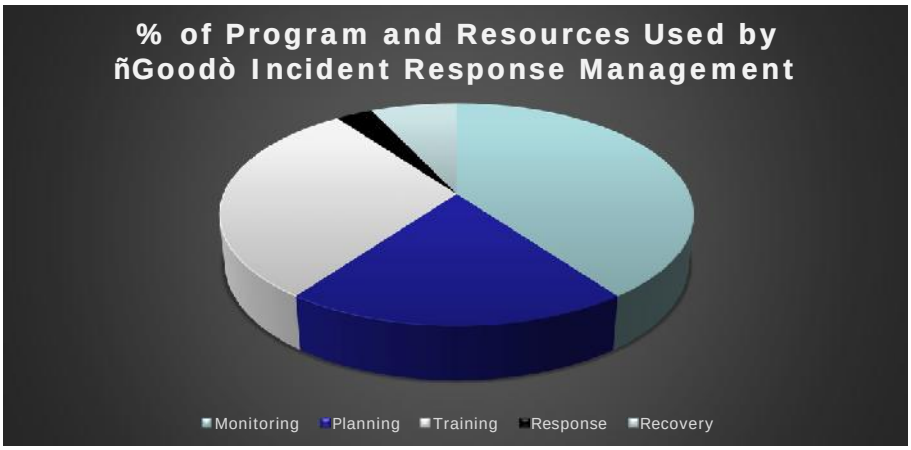
infotex
© 2014, 2015 Infotex Inc. All rights reserved.
infotex

Regulatory Framework (and thus) Security Adoption



infotex
© 2014, 2015 Infotex Inc. All rights reserved.
infotex

Incident Response:
a small part of Incident Response Management



infotex

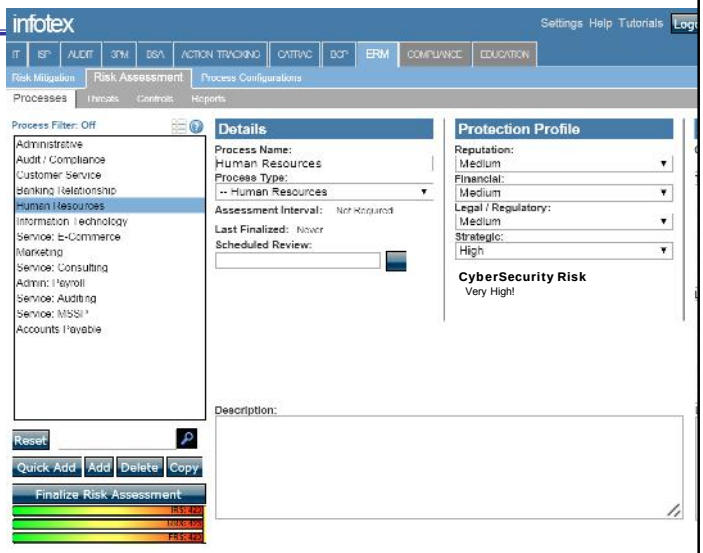
The Result

infotex

No Category

We've been trained to see major risk categories as the following:

- Reputational
- Financial
- Legal (Regulatory)
- Strategic

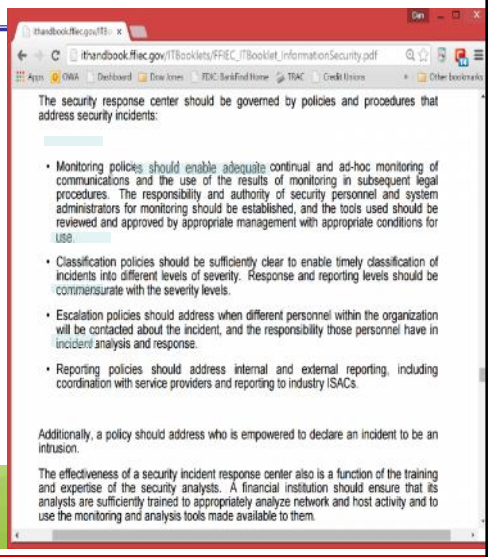


TRAC

infotex

FFIEC Guidelines

- Little specificity on definition of ñmonitoring.ò
- Heavy on response and not preparation.
- No formal requirement for training or testing.

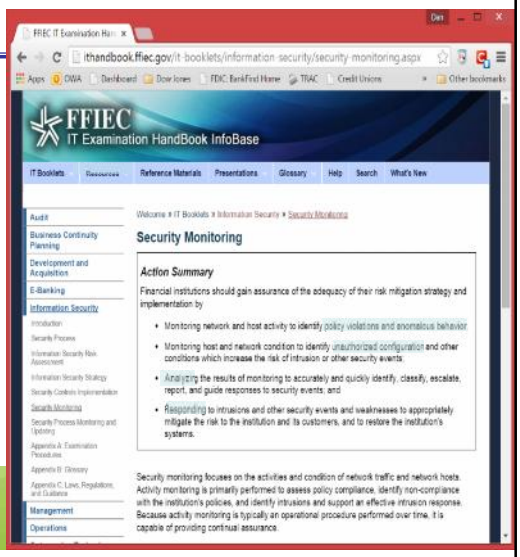


FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

infotex

Monitoring

- Weak requirements
- No specific instructions



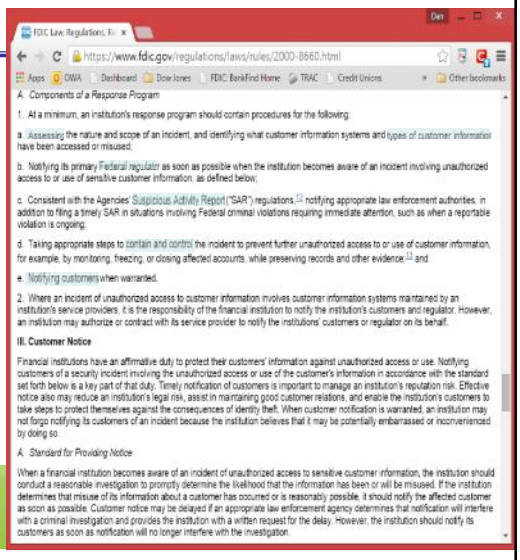
FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

infotex

Supplements

- Detect and Response is in the Supplement to the FFIECôs 2005 Guidance on Multifactor Authentication.
- Two new statements on malware and compromised credentials.

- Each regulatory agency is releasing its own set of sporadic Bulletins, FILs, and SRs.



FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

infotex

And thus . . . .

Current Programs Are:

- Auditor/Examiner Driven
- Based on FILs, Bulletins, SRs from individual agencies, as they interpret the FFIEC guidelines.
- Very non-technical, process oriented
- Does not integrate risk monitoring as a response process.

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

- FFIEC Information Security
  - Section Analysis And Response
- FFIEC Internet Banking Authentication Guidance
- FFIEC Statement on Cloud Computing
- FFIEC Statement on Credentials
- FFIEC Statement on Malware
- FFIEC Appendix J (BCP Booklet)
- FDIC Appendix B to Part 364
  - Section III Response Program
- NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide
- NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response
- BITS DDOS Guidance

infotex

And thus . . . .

Current Programs Are:

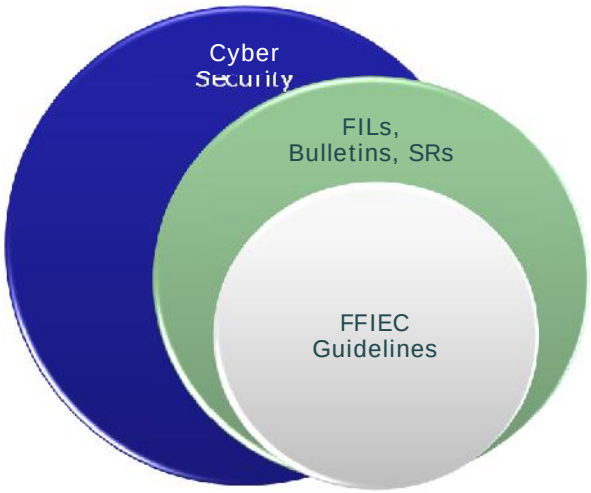
- Auditor/Examiner Driven
- Based on FILs, Bulletins, SRs from individual agencies, as they interpret the FFIEC guidelines.
- Very non-technical, process oriented
- Does not integrate risk monitoring as a response process.

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

- FFIEC Information Security
  - Section Analysis And Response
- FFIEC Internet Banking Authentication Guidance
- FFIEC Statement on Cloud Computing
- FFIEC Statement on Credentials
- FFIEC Statement on Malware
- FFIEC Appendix J (BCP Booklet)
- FDIC Appendix B to Part 364
  - Section III Response Program
- NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide
- NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response
- BITS DDOS Guidance

infotex

Missing Controls



infotex

What has been missing?

- Risk monitoring (based on accepted risk, asset value, etc.)
  - Need to monitor accepted risk AND veracity of controls
  - Threat Intelligence
- Ability to detect cyber incidents.
- Appropriate training for incident response management.

infotex

That was then, this is now!

Domain 5

Cyber Incident Management and Resilience

Cyber incident management includes establishing, identifying, and analyzing cyber events; prioritizing the institution's containment or mitigation; and escalating information to appropriate stakeholders. Cyber resilience encompasses both planning and testing to maintain and recover ongoing operations during and following a cyber incident.

Assessment Factors	
	Incident Resilience Planning & Strategy incorporates resilience planning and testing into existing business continuity and disaster recovery plans to minimize service disruptions and the destruction or corruption of data.
	Detection, Response, & Mitigation refers to the steps management takes to identify, prioritize, respond to, and mitigate the effects of internal and external threats and vulnerabilities.
	Escalation & Reporting ensures key stakeholders are informed about the impact of cyber incidents, and regulators, law enforcement, and customers are notified as required.

www.ffiec.gov/cyberassessmenttool.htm

Process Flow for Institutions:

Step 1: **Read Overview for Chief Executive Officers and Boards of Directors** to gain insights on the benefits to institutions of using the Assessment, the roles of the CEO and Board of Directors, a high-level explanation of the Assessment, and how to support implementation of the Assessment.

Step 2: **Read the User's Guide** to understand all of the different aspects of the Assessment, how the inherent risk profile and cybersecurity maturity relate, and the process for conducting the Assessment.

Step 3: **Complete Part 1: Inherent Risk Profile of the Cybersecurity Assessment Tool** to understand how each activity, service, and product contribute to the institution's inherent risk and determine the institution's overall inherent risk profile and whether a specific category poses additional risk.

Step 4: **Complete Part 2: Cybersecurity Maturity of the Cybersecurity Assessment Tool** to determine the institution's cybersecurity maturity levels across each of the five domains.

Step 5: **Interpret and Analyze Assessment Results** to understand whether the institution's inherent risk profile is appropriate in relation to its cybersecurity maturity and whether specific areas are not aligned. If management determines that the institution's maturity levels are not appropriate in relation to the inherent risk profile, management should consider reducing inherent risk or developing a strategy to improve the maturity levels.

Refer to the User's Guide for additional explanation of Steps 3, 4, and 5.

In addition to the "Overview for Chief Executive Officers and Boards of Directors", the FFIEC has released the following documents to assist institutions with the Assessment.

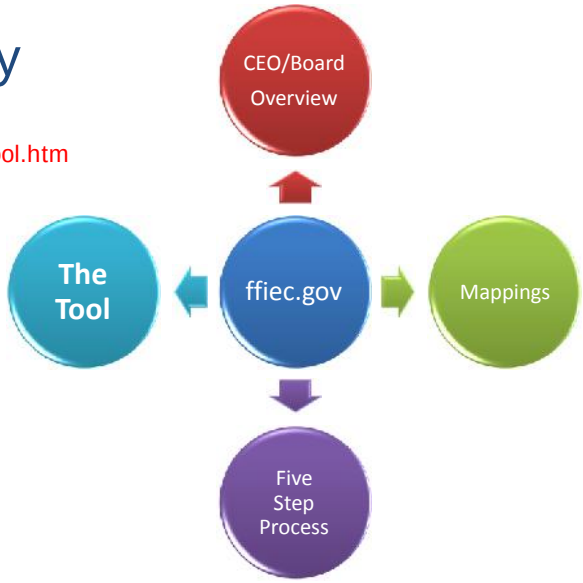
- Appendix A: Mapping Baseline Statements to FFIEC IT Handbook
- Appendix B: Mapping to NIST Cybersecurity Framework
- Appendix C: Glossary

Paperwork Reduction Act
OMB Control No. 1557-0328
Expiration Date: December 31, 2015
A Federal agency may not conduct or sponsor, and an organization (or person) is not required to respond to, a collection of information unless it displays a currently valid OMB control number

Cybersecurity

Assessment Tool

ffiec.gov/cyberassessmenttool.htm



THE TOOL:

- User's Guide
- Inherent Risk Profile
- Cybersecurity Maturity

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

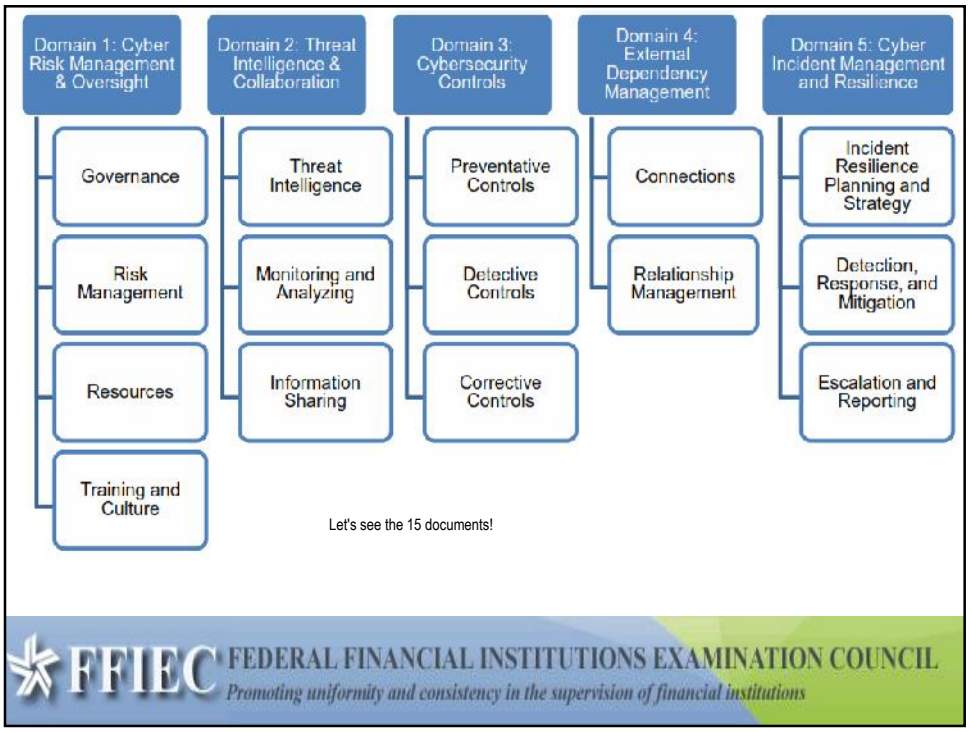
Promoting uniformity and consistency in the supervision of financial institutions

Primary Differences

1. Inventory of connections as well as other information assets.
2. Identification of information that should be encrypted at rest.
3. Testing of Incident Response Planning
4. More robust network monitoring beyond IPS/IDS on perimeter
    1. IDS on the internal network
    2. Event Log Management
    3. Change Detection on Firewall
5. Method of analyzing and responding to threats as they arise.
6. Awareness Training for the Board of Directors, Incident Response Team, and other "entities" besides our users and customers.

infotex

© 2014, 2015 Infotex Inc. All rights reserved.



NIST on NIST

https://www.youtube.com/watch?v=OVONwiWndaM

m.infotex.com/nist021914

infotex

Choosing a Framework

- PCI (laughable)
- HIPAA (Gives CyberSecurity A Nod)
- ISO and CobiT (complex)
- FFIEC Guidelines (Weak)
- NIST 800-61: (Not integrated)
- NIST CyberSecurity Framework: Almost there
- FFIECôs Cybersecurity Assessment Tool: Just Right, Goldilocks!

infotex

Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Frameworks
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

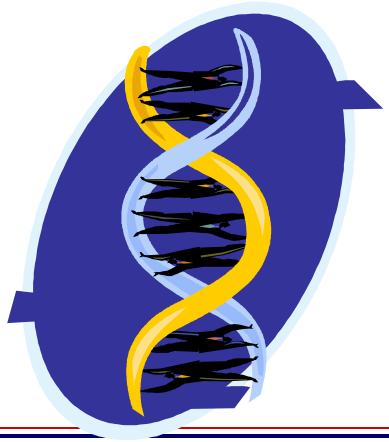
Policies and Procedures

- Codify the support Management can give to the Information Security Process.
- Act as a guideline that ensures compliance.
- Establishes rules that cross departmental barriers and enlists support of Custodians.

infotex

Policies Are a System

- They are organic . . .
- Change one, change them all!
- They interact!



infotex

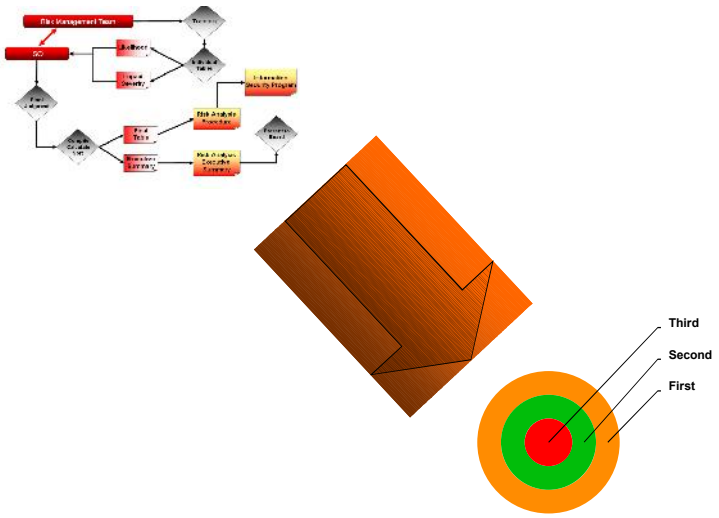
They're the beginning of a process!

Meanwhile, back in REALITY

- We work with banks as small as 50 million and as large as 2.5 billion.
- Our boilerplates attempt to address both ends of the spectrum.

KISS!

Customize to Your Bank



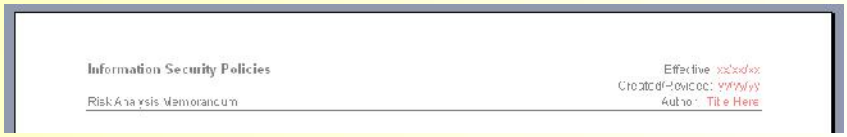
Boilerplates

- Starting points
- Suggested language
- Totally meaningless if not enforced

See policies as a strategy!

Standard Policy Template Items

- Header / Footer Information
  - Name of Policy
  - Effective Date
  - Creation / Revision Date
  - Author (or “Owner”)
  - Page Number

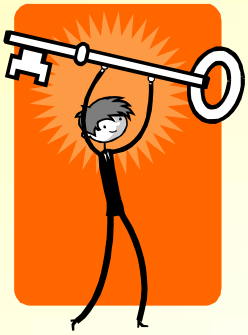


Standard Policy Template Items

- Introductory Sections
  - Scope
  - Authority
  - Introduction (background information)
  - Objectives

Standard Policy Template Items

- Concluding Sections
  - Reporting to the Board
  - Status Reporting
  - Exception Process
  - Noncompliance
  - Policy Training
  - Distribution List
  - Storage of Policy
  - Related Policies, Procedures and Tools



Boilerplate Protocols

- Red: Insert applicable name, title, policy, procedure, etc. in this spot.
- Blue: Instructions
- **Brown: Consider leaving in**
- Copyright of customized information turned over to the bank as a deliverable of this workshop.
- However, please honor spirit of proprietary nature of these boilerplates.

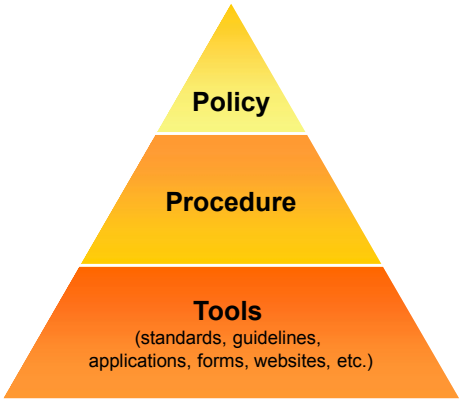
infotex

Incident Response Plan

- **Show 'em the colors in the actual word document!**

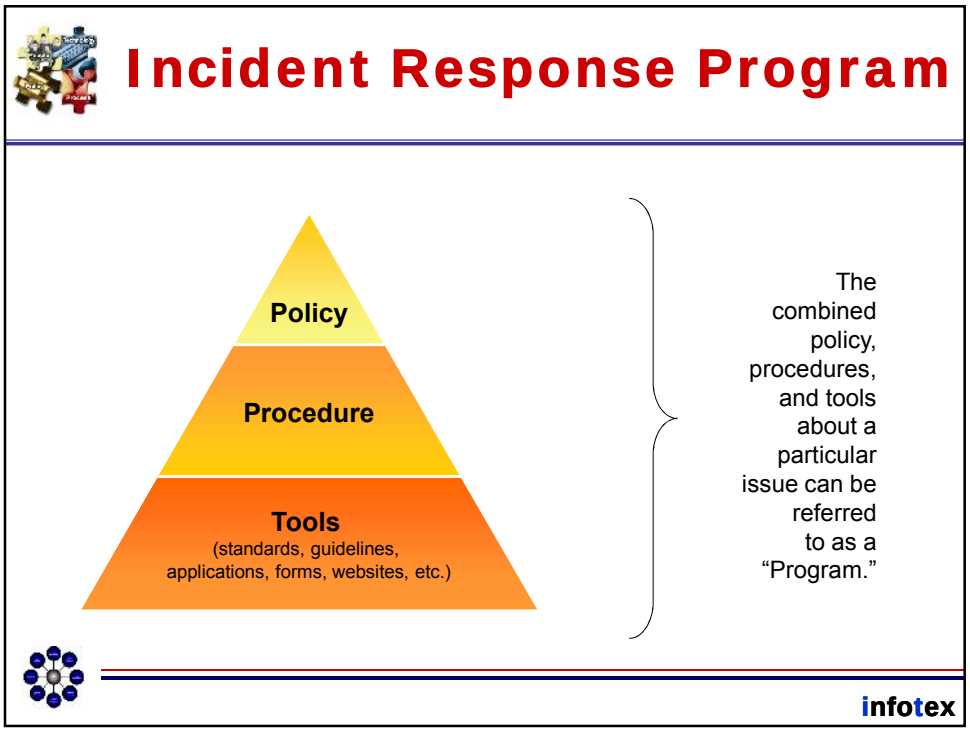
infotex

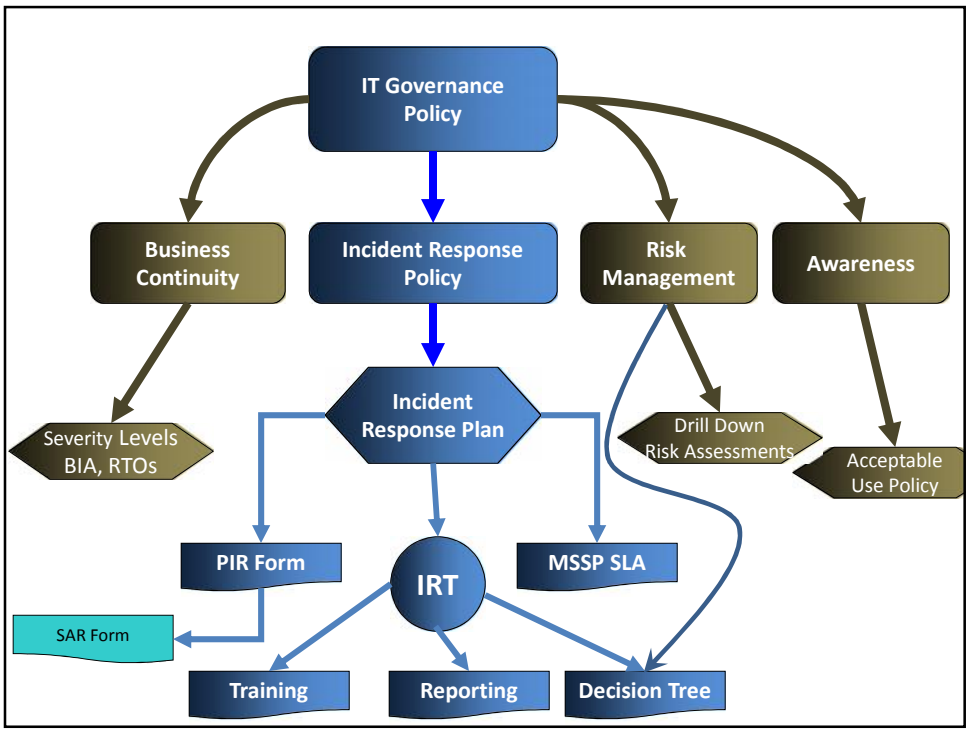
IT Governance Program

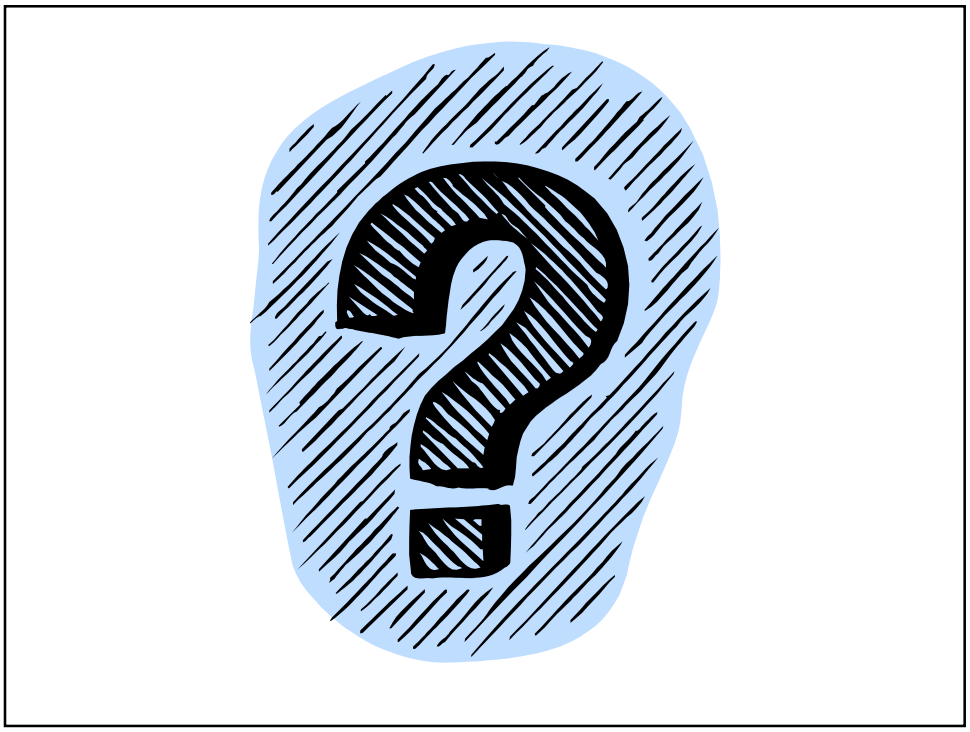


The combined policy, procedures, and tools about a particular issue can be referred to as a "Program."

infotex


Incident Response Program
Policy
Procedure
Tools
(standards, guidelines, applications, forms, websites, etc.)
The combined policy, procedures, and tools about a particular issue can be referred to as a "Program."
infotex


IT Governance Policy
Business Continuity
Incident Response Policy
Risk Management
Awareness
Severity Levels BIA, RTOs
Incident Response Plan
Drill Down Risk Assessments
Acceptable Use Policy
PIR Form
IRT
MSSP SLA
SAR Form
Training
Reporting
Decision Tree



Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Framework
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

See Incident Response As . . .

Choosing a Framework

- PCI (laughable)
- HIPAA (Gives CyberSecurity A Nod)
- ISO and CobiT (complex)
- FFIEC Guidelines (Weak)
- NIST 800-61: (Not integrated)
- NIST CyberSecurity Framework: Almost there
- FFIECôs Cybersecurity Assessment Tool: Just Right, Goldilocks!

infotex

How do you articulate it?

- Do you choose a framework now, or wait to see if there is a guidance?
- Do you choose the FFIEC Guidelines, the NIST 800-61, the NIST CyberSecurity Framework, or the FFIEC Assessment Tool?

infotex

High Level View of Policy

- Objective, Framework, Goals
- Team Membership, Training, Testing
- Thou shalt create an Incident Response Program
- Meeting Requirements
- Types of Incidents
- Notification

Typical Membership

- IT and Information Security Of Course
- Network Administrator(s)
- Executives (could be CEO/President in smaller organizations, try to get as high as possible in larger organizations.
- Marketing: whoever is the "authority" on public relations
- Human Resources: who wants to handle insider issues?

A-typical Membership

- Legal Counsel
- The MSSP (usually a person who can decipher the reports)
- Your Network Support Provider

Guest Speakers

- MSSP
- Law Enforcement
- Examiners and Regulators
- Auditors (especially for audits that involve incident response, such as social engineering tests and network penetration tests.)

Figure 2-1. Communications with Outside Parties

Incident Definitions

- Disclosure Incident
- Security Incident
- Negative Incidents

infotex

Disclosure Incidents

- Incidents which, because of some statute or regulation, or just doing the right thing, require you to notify customers, law enforcement, examiners, or the board of directors.

infotex

Security Incidents

- Incidents related to the confidentiality and integrity of information.

infotex

Security Incidents

- They can include technical incidents such as malware (virus, worm, and Trojan horse) detection, unauthorized use of computer accounts and computer systems,
- They can also include non-technical incidents such as improper use of information assets as outlined in the Acceptable Use Policy.

infotex

Negative Incidents

- These are incidents related to the availability of information assets or other risks such as legal risks, strategic risks, or reputational risks that do not directly impact the confidentiality or integrity of information.

infotex

Negative Incidents

- For example, installing an unlicensed application on a bank-owned application does not impact confidentiality, integrity, or availability, but the policy still requires the Incident Response Team to track it.

infotex

Optional Severity Rating

- Our policy boilerplate is now making the assignment of severity ratings optional.
- Larger banks (>500 million) should probably still do this.
- Smaller banks, see what your auditors/examiners think.

infotex

Very Important Language:

- The Information Security Officer is authorized to declare Incident Types and Incident Severities.

infotex

Boilerplate

Purpose

- This is a "template" to be used as a "starting point" for the sake of helping you develop your own IT Governance Program.

Copyright / Permission to Use

- Permission to use this document is conditional upon you receiving this template directly from an **infotex** consultant, **infotex** website or e-commerce site, or an **infotex** workshop / training presentation.
- By using this template either in its entirety or any portion thereof, you acknowledge that you agree to the terms of use as dictated in the "Transfer of Copyright Agreement" located at copyright.**infotex**.com. This agreement establishes that when you customize this template to your specific needs, your organization may have copyright of the customized document. However, **infotex** retains copyright to the template. This agreement also establishes that you will not share this or any other template with third parties other than auditors and examiners. You may not transfer ownership of the customized documents to any other organization without the express written permission of **infotex**.

Instructions

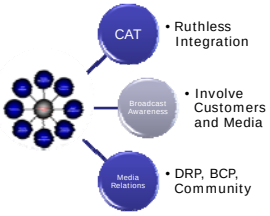
- Make sure to read through the template carefully as not all situations will pertain to your organization. However, to assist you in customizing the document to your specific needs, we have attempted to color code areas that will need your special attention. Color coding is as follows:
  - All areas needing customization and/or consideration are in **red**.
  - Sections that are in **brown** are optional sections according to our definition of best practices. These sections may be removed if they do not match your needs.
  - Sections in **blue** are merely instructions or additional information for knowledge purposes and should be removed.
  - Sections in **green** are examples.
- Note that you should confirm that all text has been changed to "black" before considering this template final for your organization. If there are any sections in any other color than black, then all situations or customization has not been considered.
- This section (Templates) may be removed once the document has been customized, for at that time we turn ownership of the customized document over to you.

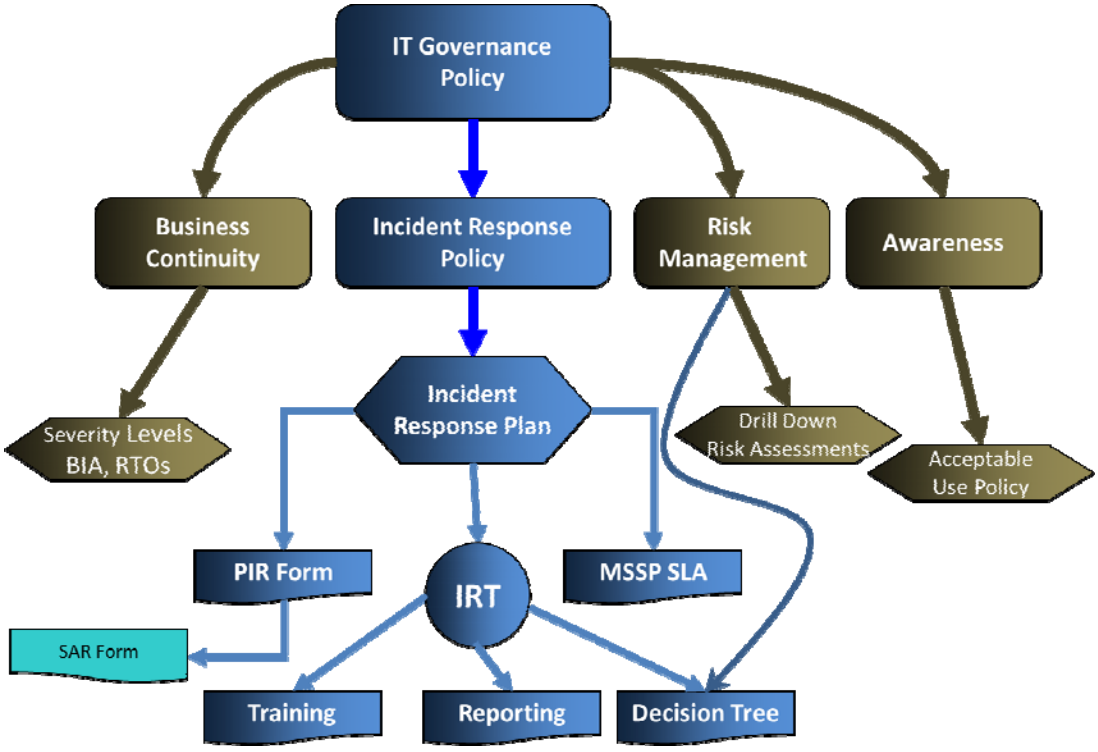
© Copyright 2000 - 2015 **infotex**, Inc. All rights reserved.

NOTES ABOUT THIS BOILERPLATE:

- The Incident Response Policy is a "board-level" policy that gives birth to a program which is very closely related to the Business Continuity Program.
- Many smaller banks will make the Incident Response Team congruent with, if not a subset of, the Business Continuity Team, or they use a steering committee with HR and Marketing.
- The bank should consider adding to a high-level, management-wide policy, the following language:
- This document does not yet (as of 08/22/15) integrate implications of the Cybersecurity Assessment Tool. Look for new documents to be available in 2016! For this iteration, anything related to the tool has been highlighted in yellow.

"Management will inform the Incident Response Team any time a new technology is deployed, any time a new product or service is deployed, and/or any time a major system is updated."





Iterations:

Iteration #: 7
Date of This Iteration: 12/08/2011
Original Iteration: September 2002

Iteration #: 8
Date of This Iteration: 06/04/2015
Original Iteration: September 2002

- Included testing in the policy.
- Added additional Scenario Standards documents, (DDoS, Vendor Breach, Phishing Attack, Malware Breach, Social Engineering Attack, etc.) and called for them in the plan.
-

Iteration #: 9
Date of This Iteration: 06/30/2015
Original Iteration: September 2002

- Addressed the Cybersecurity Assessment Tool at a high level by:
  - Requiring it to be considered during plan development.
  - Requiring management to determine appropriate maturity levels for incident response processes (primarily Domains 2, 3, and 5) based on inherent risk.
  - Requirements that Domain 5 be brought to an <advanced, innovative> maturity level for larger banks.
  - Note that while it is tempting to realign the entire policy with the Cybersecurity Assessment Tool, we believe you should still adopt language requiring you to comply with your agency's articulation of customer notification requirements, especially if your state law allows you to defer to federal regulations in the event of customer notification.
  - Given this is very new, language has been highlighted.

Next Update Due: 08/26/15

Known Changes for Next Update:

- Will include a more thorough review of the Cybersecurity Assessment Tool and align with an updated Plan based on the tool.
- Will add additional scenarios to plan (Compromised Credentials)
- Will make sure Virus Incident Response Procedures conforms to FFIEC Statement on Destructive Malware.

ONE PAGE POLICY MINIMUM:

Some of our Clients have a one page (or less) policy statement inserted into their high level governance policy, and then call our "policies" procedures, and our "procedures" standards. The following is the "minimum language" to facilitate the "one page policy statement."

Incident Response:

The Federal Financial Institutions Examination Council (FFIEC) indicates that the IT operations management should implement corrective (incident response) security controls. The [CIRT / IRT / Steering Committee / Information Security Officer] will create and maintain an Incident Response Program that establishes an Incident Response Procedure as well as an Incident Response Plan. The Incident Response Procedure will articulate the details of enforcing this policy, whereas the Incident Response Plan will address goals and priorities, making life and safety the highest priority, as well as articulate a process for responding to incidents.

Management will form an Incident Response Team, and the Information Security Officer will be responsible for training that team to meet responsibilities articulated in this policy and the Incident Response Procedure. These responsibilities will include participation in a monthly Incident Response Team Meeting as well as being available for emergency meetings, reading and learning the Incident Response Program, and participating in incident response tests.

The board wants all incidents to be classified as follows:

- Disclosure Incidents: These are incidents which, because of some statute or regulation, require [name of financial institution] to notify customers, law enforcement, examiners, or the board of directors. The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] must comply with all applicable laws and regulations, including state laws such as [Indiana Code 24-9.4 / applicable law in your state] and federal regulations such as the [FDIC's Financial Institution Letter 27-2005, the OCC Supervisor Letter 2005-13, for Fed and NCUA institutions ---> the FFIEC's Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice] and/or any other applicable guidance or regulations as they are developed.
- Security Incidents: These are incidents related to the confidentiality and integrity of information. They can include technical incidents such as malware (virus, worm, and trojan horse) detection, unauthorized use of computer accounts and computer systems, but can also include non-technical incidents such as improper use of information assets as outlined in the Acceptable Use Policy.
- Negative Incidents: These are incidents related to the availability of information assets or other risks such as legal risks, strategic risks, or reputational risks that do not directly impact the confidentiality or integrity of information. For example, installing an unlicensed application on a bank-owned application does not impact confidentiality, integrity, or availability, but this policy still requires the [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] to track it.

The board should be informed of incidents in the Annual Information Security Report to the Board as required by the FFIEC guidelines, and whenever an incident is classified as a Disclosure Incident the board should be notified "in real time." The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] should also determine our maturity level for Cybersecurity Assessment Tool Domains 2, 3, and 5, and included in the report when we are not at an

advanced or innovative maturity level. Critical Incidents should be formally closed, and the report should identify any open incidents. The Incident Response Program should be tested on an annual basis at least twice, and one of the tests should be of a scenario which would be classified as a "Disclosure Incident." Tests should include a test plan, minutes of the actual test, and documentation of a "post-mortem review." Test results should be presented to the board.

Insert Financial Institution Name / Logo

Incident Response Policy

(Approved During DD/MM/YY Board Meeting)

Classified: Confidential Information
Contact if found: Name, Title
Name of Financial Institution
City, State

Policy Scope

This policy applies to all Name of Financial Institution's employees, temporary workers, contractors, and consultants who use and modify Name of Financial Institution's computer resources.

The Board of Directors and the Information Security Officer is responsible for overseeing the development, implementation, and maintenance of this policy. It should be reviewed at least annually to ensure relevant information is appropriately considered.

The Incident Response Team is responsible for enforcing this policy.

For questions concerning this policy, see the Information Security Officer.

Introduction

Given the risk-based approach to Information Security and that there is no such thing as 100% security, implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents. The number of computer security incidents and the resulting cost of business disruption and service restoration must be monitored and measured.

Intrusion detection plays an important role in implementing and enforcing an organizational Incident Response Policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems, some type of assurance is needed that indicates the systems and networks are secure. Intrusion detection systems can provide part of that assurance.

The Federal Financial Institutions Examination Council (FFIEC) indicates that the IT operations management should implement corrective (incident response) security controls. This provides a framework for IT operations information security. *Referenced in FFIEC Information Operations Booklet.*

Objective

To comply with the Information Technology Governance Policy, this document creates the [creates the Computer Incident Response Team ([Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team]) and establishes the membership, roles, responsibilities, and authority of the [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team]. / creates the Incident Response Team (IRT) and establishes the membership, roles, responsibilities, and authority of the IRT / assigns the responsibility for Incident Response to the existing Technology Steering Committee / etc]. In addition, it requires the creation of an Incident Response Program for dealing with incidents related to technology and information risk. Such incidents include incidents which require certain notifications by law, security incidents, and negative incidents arising because of technology and information risk. For the sake of "disclosure incidents" defined herein, we must enforce the regulations articulated in the [FIL 2005-27 | OCC Bulletin 2005-13 | Interagency Guidelines 05-05980 | Appendix B of Part 364 on FFIEC.gov] as well as other federal

regulations as applicable.

Goals and Priorities

The Board of Directors requires that management establish and maintain an Incident Response Program that meets the following incident response management objectives:

- Establish and train a multi-disciplinary Incident Response Team.
- Establish and maintain a risk monitoring process that will allow early detection of incidents
- Establish and maintain a method of "broadcasting awareness" when appropriate
- Create and maintain an event classification system that facilitates a simple, effective "triage process."
- Monitor accepted information security risk and technology risk.
- Establish an "audit framework" that can be used to determine the maturity level of our Incident Response Program. For this revision of the program, we are using the [NIST CyberSecurity Standard / FFIEC Guidelines / Other framework] as our framework.

[Name of Financial Institution] has created the [Computer Incident Response Team ([Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team])] to develop and maintain an Incident Response Program. The Incident Response Program should be designed with the following goals in mind:

- Proactive Goals:
- Reactive Goals
- Reactive / Proactive Goals

The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] should also develop and implement the Incident Response Program with the following priorities as a basis:

1. Protect human life and safety.
2. Protect customer information and assure organizational data integrity.
3. Maintain the financial institution's reputation and control external communication.
4. Prevent damage to systems.
5. Minimize disruption of computing resources.

Though for the purposes of creating an incident response process we will not include these types in our classification structures, it is helpful to know that the following types of negative actions can be considered to be a "technology incident."

- Increased Access
- Disclosure of Information
- Corruption of Information
- Denial of Service
- Theft of resources
- Negative Reputation
- Negative Legal Implications

Definition of Customer Information:

According to guidance, sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account numbers.

[Computer Incident Response Team (CIRT) / Incident Response Team (IRT) / Steering Committee Membership]

Note: Most banks now call this team the "Incident Response Team" because this policy governs more than just computer incidents. Smaller banks assign the responsibility normally assigned to an Incident Response Team to existing committees, such as the Technology or the IS Steering Committee.

The following personnel have been designated as members of the [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team]:

- Information Security Officer (Team Leader)
- BSA Officer
- Security Officer
- Disaster Recovery Coordinator
- Marketing Coordinator / Customer Relations Officer
- Chief Information Officer / VP IT / IT Director
- Compliance Officer / Internal Auditor
- Human Resources Director
- Information Systems Manager / Network Administrator

In addition, the following third parties may be involved in [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] meetings, as needed:

- Managed Security Provider
- Network Service Provider

Note: The FFIEC requires a multi-disciplinary incident response team. Many banks simply add Human Resources and Marketing (Public Relations) to their existing IS Steering Committee. Smaller banks may already have this membership on the IS Steering Committee (as the bank's President handles the "marketing/public relations" aspects of response.)

Incident Response Program

The [CIRT / IRT / Steering Committee / Information Security Officer] will create and maintain an Incident Response Program that establishes an Incident Response Plan and necessary ancillary procedures and tools that serve as guidelines for an overall approach to incidents.; establishes processes for containment, eradication, recovery, and follow-up on incidents; includes a severity rating assignment process for various incident types; documents notification requirements establishing guidelines for

reporting incidents as well as regular reporting requirements for summary reports to Management and the Board of Directors; and includes provisions for documentation of critical information necessary in the event of an incident. Finally the plan will include guidelines for IT personnel and users at-large to report observed suspicious activity.. The Incident Response Plan will address goals and priorities, making life and safety the highest priority, as well as articulate a process for responding to incidents. The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] should also determine our maturity level for Cybersecurity Assessment Tool Domains 2, 3, and 5, and the Annual Information Security Report to the Board should articulate when we are not appropriately aligning maturity of controls with inherent risk. The entire Cybersecurity Assessment Tool should be considered when developing the Incident Response Plan. Management should determine appropriate maturity levels for incident response processes expressed in Domains 2, 3, and 5; and report when our maturity level cannot be brought to an appropriate state (advanced or innovative.) Anywhere we fall below the prescribed baselines should also be reported. The board requires that Domain Five be brought to and maintained at an [advanced / innovative] maturity level.

Meeting Requirements

The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] will meet [monthly / quarterly / on a periodic basis]. The Information Security Officer will prepare an agenda for and keep the minutes of this meeting. Regular reporting requirements will be reviewed in each meeting, as well as proposals to update the Incident Response Program as needed. The Information Security Officer will also provide necessary ongoing training related to Incident Response in these meetings.

It is imperative that all members of the [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] be available at all times for emergency [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] meetings, and are given appropriate training to investigate and report findings. The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] should have access, if necessary, to back-up data and systems, an inventory of all approved hardware and software, and monitored access to systems, as appropriate. The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] must also have timely access to decision makers for actions that require higher approvals.

Clasification of Incidents into Types

The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] will classify all incidents into one of three Types:

- Disclosure Incidents: These are incidents which, because of some statute or regulation, require [name of financial institution] to notify customers, law enforcement, examiners, or the board of directors. The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] must comply with all applicable laws and regulations, including state laws such as [Indiana Code 24-9.4 / applicable law in your state] and and federal regulations such as the FDIC's Financial Institution Letter 27-2005, the OTS CEO Memo – Data Breaches of March 2005, the OCC 2005-13, and any other applicable guidances or regulations as they are developed.

- Security Incidents: These are incidents related to the confidentiality and integrity of information. They can include technical incidents such as malware (virus, worm, and trojan horse) detection, unauthorized use of computer accounts and computer systems, but can also include non-technical incidents such as improper use of information assets as outlined in the Acceptable Use Policy.
- Negative Incidents: These are incidents related to the availability of information assets or other risks such as legal risks, strategic risks, or reputational risks that do not directly impact the confidentiality or integrity of information. For example, installing an unlicensed application on a bank-owned application does not impact confidentiality, integrity, or availability, but this policy still requires the [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] to track it.

The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] may develop a severity classification system within each incident type. The Information Security Officer to report all Notification Incidents to the Board of Directors as they occur, and report [severe / critical] Security Incidents and [critical / severe] Negative Incidents as deemed necessary by the [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] in real time.

The Information Security Officer is authorized to classify incident types, as defined above, as well as incident severities. All incidents should be summarized by type and [criticality / severity] in the Annual Report to the Board. This report should include status information for all "disclosure incidents."

Be sure the following two sections (Incident Severity and Notification) equal your policy.

Definition of "Real Time"

The Incident Response Policy requires the Information Security Officer to keep the Board of Directors informed, in "real time," during Disclosure Incidents. For the purposes of policy compliance, we define "real time" as a steady stream of information provided as needed and reasonable, at the Information Technology Committee's discretion, as it determined to be appropriate. To clarify, while the Board may be updated "in real time," customers are rarely notified in real time, because we do not know if the information is complete and accurate.

Incident Severity

The Information Security Officer will create a severity assignment process for all incidents. The Information Security Officer will assign one of three severity ratings to incidents as they are reported.

1) [Minor / Trend] Incident: This incident is low risk and, though should be monitored and reported in an upcoming [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] meeting, does not warrant immediate action or reporting.
2) [Critical / Severe / Emergency] Incident: This incident requires an emergency [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] Meeting to determine response actions, notification requirements, etc.
3) Disaster (Availability) Incidents: This incident requires execution of the Disaster Recovery Plan, and will defer to response processes and severity ratings in that plan. . . . or . . .

Disaster Incidents: Some incidents require execution of the Business Continuity Plan, and will defer to response processes and severity ratings in that plan, as decided by the Information Security Officer.

Incident Response Tests

The Information Security Officer will plan for and coordinate testing of the Incident Response Program. These tests should be conducted on an annual basis at least twice, and one of the tests should be of a scenario which would be classified as a "Disclosure Incident." All Incident Response Team members should attend the tests. Tests should include a test plan, minutes of the actual test, and documentation of a "post-mortem review." Test results should be presented to the board. A walk-through test should be conducted when the plan is updated. A tabletop test should be conducted against a high likelihood "incident scenario." Functional tests, conducted during social engineering portions of audits or internally, should also be conducted.

Broadcast Awareness

The Information Security Officer will create, publish, and maintain a process for quickly moving through "triage" on new incidents. This process will be named "Broadcast Awareness," and should be addressed in the Acceptable Use Policy as well as in annual awareness training. Whenever possible, the time to broadcast awareness should be measured in tests and incidents.

Triage

The Information Security Officer will create, publish, and maintain a process for determining the scope and nature of an incident, resulting in the classification, documentation, and escalation (if necessary) of the incident in a timely manner. This process will be documented in the Incident Response Pan.

When Customer Notice is required

Note that while it is tempting to realign the entire policy with the Cybersecurity Assessment Tool, we believe you should still adopt language requiring you to comply with your agency's articulation of customer notification requirements, especially if your state law allows you to defer to federal regulations in the event of customer notification.

The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] must comply with all applicable laws and regulations, including state laws such as [Indiana Code 24-9.4 / applicable law in your state] and federal regulations such as the FDIC's Financial Institution Letter 27-2005, the OCC 2005-13, and any other applicable guidance or regulations as they are developed. Guidance maintains that <Name of Financial Institution> must notify customers whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur.

Notification Tactics

The Incident Response Plan will document how we are to notify customers, according to guidance.

Compliance steps to Following during a Disclosure Incident

Guidance maintains that the following steps be followed in an Incident Response:

1. Triage: Assess nature and scope of incident and determine if customer notification is required. (Determine Disclosure Requirements)
2. Notify your federal regulator.
3. File a timely SAR.
4. Contain and Control
5. Notify Customer

We will of course contain an incident as a first priority. The above identifies the compliance steps that must be followed in an incident.

Post-mortem [Post Incident] Review

Note: Many institutions will move this to the plan and not have it as part of the policy. We feel this is a mistake as we audit organizations that never get to the post-mortem review. For all incidents and incident response tests, the Incident Response Team will conduct a "Post-Mortem Review" within a reasonable amount of time after the incident. This review can be conducted as far as the "Incident

Closure Process," but should be conducted shortly after an incident even if the incident is not closed. It can be conducted in the first Incident Response Team Meeting after an incident.

In the post-mortem review, the following questions should be asked and answered:

- Exactly what happened, and when?
- How long did it take for us to "broadcast awareness"
- What caused it?
- How long did it take to contain the incident?
- How long did it take for us to eradicate the incident?
- How long did staff and management perform in dealing with the incident?
- Were the documented procedures followed?
- Were they adequate?
- What corrective actions can prevent similar incidents in the future?
- What lessons did we learn?

Board Notification

Note: Most "Disclosure Incidents" will warrant "real-time disclosure" to the board. However, some disclosure incidents, such as CAMS alerts from vendors, may be reported to the board in a normal meeting cycle. Still, the Information Security Officer should consider these to be

The Information Security Officer will notify the Board of Directors of all Disclosure Incidents "in real time." The Board of Directors will also be notified "in real time" anytime an incident is considered to be critical in severity. Disclosure incidents not considered critical (such as some CAMS Alerts) will be reported to the board monthly.

All suspected and/or confirmed instances of attempted and/or successful intrusions must be immediately reported according to the Incident Response Plan. The Incident Response Plan will address regular reporting requirements for analyzing trends, performing "post-mortem analysis" of past incidents, and other requirements as determined by the [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team].

The [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] will create and document Notification Requirements in the Incident Response Plan that establishes guidelines for reporting incidents to management, to the Board of Directors, to law enforcement, to customers, and to the media in a manner consistent with all applicable laws as well as the bank's risk management policies and procedures.

Incident Closure

It is very important that we make sure we BENEFIT from what we can learn from an incident. We've taken the impact of the incident, let's try to turn it into some value for the institution.

Thus the incident closure process is very important. All incidents that are classified as [Critical / Severe / Emergency] or as Disaster (Availability) Incidents must be formally closed by the Incident Response Team.

Open incidents should be identified in the Annual Information Security Report to the Board.

Risk Monitoring

The Information Security Officer will ensure that the Incident Response Team is monitoring accepted risk. When the Board of Directors accepts the risk on various information assets, this acceptance is based upon the understanding that the Incident Response Team is monitoring for a threat exploiting a vulnerability for known accepted risks. The Incident Response Team will be responsible for monitoring non-technical risk. The Information Security Officer may outsource, with Board approval, the monitoring of some technical risk. The Board of Directors requires that the Incident Response Team adopt [the NIST CyberSecurity Framework | NIST SP 800-61 | the FFIEC Guidelines] as the framework for which Risk Monitoring will be audited against. The Information Security Officer will inventory and/or diagram layers of risk monitoring controls.

Concluding Sections

The following sections may or may not apply to your institution, depending upon your own policy/procedure development protocols. However, we do strongly urge you to include the distribution list, policy owner, and policy reviewers section for your convenience and to ensure appropriate review and training. Please remove this section.

Review

This policy will be reviewed annually to ensure that it is kept current to existing technology and knowledge about Information Security. Meanwhile, tools (such as the IDS system, the signatures used, documentation, reports, logs, etc.) will be reviewed quarterly to ensure appropriateness and that they are working properly.

Due Diligence

The Information Security Officer is responsible for creating and executing a due diligence process to ensure that this policy is being enforced. All other employees will be required to funnel materials gathered as a part of this policy to the Information Security Officer for processing. The Information Security Officer will also be responsible for gathering annual documentation as required by this policy, and working with the Internal Auditor to ensure policy enforcement.

Status Reporting

The Information Security Officer must report to the Board of Directors on a semi-annual basis the status and enforcement of this policy, Information Security Program, and other Board-level policies.

Noncompliance

Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; or dismissal for interns. Additionally, individuals are subject to loss of financial institution information resources access privileges, and civil and/or criminal prosecution.

Policy Training

The Information Security Officer, Network Administrator, and Senior Management will review this policy and its associated procedures annually and hold training to ensure that everybody understands the provisions of this policy, as well as the implications upon their job description responsibilities.

Distribution List

The following positions will receive this policy and any changes to this policy:

- Board of Directors
- Information Security Officer
- All members of the [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team]
- List other individuals. Consider establishing an e-mail alias corresponding to the individuals.

Storage of Policy

The active copy of this policy will be stored in the [list location of policy].

Note: We recommend that the Financial Institution develop a method of off-site, on-line, secure storage of policies and procedures such as in a portal, mirrored intranet site, etc.

Compliance with CobiT

- Planning and Preparation
  - Creating Policies, acquiring management support, developing user awareness, building a response capability
- Detection, triage, and investigation
  - Defining events versus incidents versus notification processes
  - Detecting and validating incidents
  - Prioritizing and rating incidents
  - Implementing Intrusion Prevention, Detection, and SIEM
  - Utilizing Anti-malware and Vulnerability Management Systems
  - Conducting and participating in Global Incident Awareness
  - Conducting Log and Audit Analysis
- Containment, Analysis, Tracking and Recovery
  - Executing a containment strategy for various types of incidents
  - Performing forensics analysis according to evidence-handling processes
  - Executing Recovery Procedures in line with BCP and DRP
  - Determining source of the incident
- Post-incident Assessment
  - Conducting Post-mortem
    - Exactly what happened, and when?
    - How long did staff and management perform in dealing with the incident?
    - Were the documented procedures followed?
    - Were they adequate?
    - What corrective actions can prevent similar incidents in the future?
  - Reporting on Incident Management Related Metrics
    - Time to Broadcast Awareness
    - Mean-time to Incident Recovery
    - Cost of Recovery
  - Document Lessons Learned
- Incident Closure
  - Conducting Incident Response Post-mortem
  - Submitting reports to management and stakeholders

FFIEC GUIDELINES

See http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/appendix-d-managed-security-service-providers.aspx for a complete guidance on performing due diligence on managed security service providers.

SOURCE: FFIEC INFORMATION SECURITY BOOKLET

Page 17: Financial institutions should develop a strategy that defines control objectives and establishes an implementation plan. The security strategy should include

- [Excerpt] Appropriate consideration of prevention, detection, and **response** mechanisms.

Page 18: Security strategies include prevention, detection, and response, and all three are needed for a comprehensive and robust security framework. Typically, security strategies focus most resources on prevention. Prevention addresses the likelihood of harm. Detection and **response** are generally used to limit damage once a security breech has occurred. Weaknesses in prevention may be offset by strengths in detection and **response**.

Page 27: Passwords that are either not changed or changed infrequently are known as static pass-words. While all passwords are subject to disclosure, static passwords are significantly more vulnerable. An attacker can obtain a password through technical means and through social engineering. Internet banking customers are targeted for such social engineering through phishing attacks. Institution employees and contractors may be similarly targeted. Static passwords are appropriate in systems whose data and connectivity is considered low risk, and in systems that employ effective compensating controls such as physical protections, device authentication, mutual authentication, host security, user awareness, and effective monitoring and rapid **response**.

Page 37: Security personnel and network administrators have related but distinct responsibilities for ensuring secure network access across a diverse deployment of interconnecting network servers, file servers, routers, gateways, and local and remote client workstations. Security personnel typically lead or assist in the development of policies, standards, and procedures, and monitor compliance. They also lead or assist in **incident-response** efforts. Network administrators implement the policies, standards, and procedures in their day-to-day operational role.

Page 53: Detection devices, where applicable, should be utilized to prevent theft and safeguard the equipment. They should provide continuous coverage. Detection devices have two purposes—to alarm when a response is necessary and to support subsequent forensics. The alarm capability is useful only when a **response** will occur.

Page 76: Financial institutions should exercise their security responsibilities for outsourced operations through

- [Excerpt] Coordination of **incident response policies** and contractual notification requirements.

Financial institutions should evaluate the following security considerations when selecting a service provider:

- [Excerpt] Clear understanding of the provider's **security incidence response policy** and

assurance that the provider will communicate security incidents promptly to the institution when its systems or data were potentially com-promised.

Page 79: Financial institutions use insurance coverage as an effective method to transfer risks from themselves to insurance carriers. Coverage is increasingly available to cover risks from security breaches or denial of service attacks. Several insurance companies offer e-commerce insurance packages that can reimburse financial institutions for losses from fraud, privacy breaches, system downtime, or **incident response**.

Page 81: Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by

- Monitoring network and host activity to identify policy violations and anomalous behavior;
- Monitoring host and network condition to identify unauthorized configuration and other conditions which increase the risk of intrusion or other security events;
- Analyzing the results of monitoring to accurately and quickly identify, classify, escalate, report, and guide responses to security events; and
- **Responding to intrusions** and other security events and weaknesses to appropriately mitigate the risk to the institution and its customers, and to restore the institution's systems.

Page 91: The effectiveness of a security **incident response** center also is a function of the training and expertise of the security analysts. A financial institution should ensure that its analysts are sufficiently trained to appropriately analyze network and host activity and to use the monitoring and analysis tools made available to them.

Page 93: Successful implementation of any response policy and procedure requires the assignment of responsibilities and training. Some organizations formalize the response program with the creation of a **computer security incident response team** (CSIRT). The CSIRT is typically tasked with performing, coordinating, and supporting responses to security incidents. Due to the wide range of technical and nontechnical issues that are posed by an intrusion, typical CSIRT membership includes individuals with a wide range of back-grounds and expertise, from many different areas within the institution. Those areas include management, legal, public relations, as well as information technology. Other organizations may outsource some of the CSIRT functions, such as forensic examinations.

SOURCE: FFIEC OPERATIONS BOOKLET

Page 17: The scope of required procedures depends on the size and complexity of the institution's IT operations and the variety of functions performed by IT operations. Examples of activities or functional areas where written procedures are appropriate include:

- [Excerpt] Problem management or **incident response**;

Page 22: IT operations management should implement preventive (e.g., access controls), detective (e.g., logging), and corrective (e.g., **incident response**) logical security controls. All three types of controls provide a framework for IT operations information security. These controls can be implemented by administrative (e.g., policy), logical (e.g., access controls), or physical (e.g., locked room) controls.

Page 33: The event/problem management process should be communicated and readily available to all IT

operations personnel. Appropriate personnel—from IT operations, institution management, internal audit, fraud and loss prevention, information security, and **computer security incident response teams**—should participate in the event/problem management process.

Page 34: *Logging Issues*. Most problem-solving techniques in an IT operations center depend on the ability to read, consolidate, and interpret various operations logs. Consequently, an institution should not destroy or modify its logs. Disclosure of log tampering or manipulation is an event that requires management resolution and the involvement of the **computer incident response team**. Operations management should periodically review all logs for completeness and ensure they have not been deleted, modified, overwritten, or compromised.
Database Operations. Although various security devices protect databases, it may be possible for the operator to use system utilities or unauthorized compilations to modify the system. In such cases, the database may become corrupt or inaccessible. Operations management should regularly and carefully review all logs involving database programs and files and should report all unauthorized modifications to the **computer incident response team**.

Run Time Anomalies. Management, a shift supervisor, or another independent person should review run time logs, identify any anomalies, and review their cause and resolution. It is possible for computer operators to run programs out of sequence or with improper inputs to cause error or fraud. Automated scheduling programs commonly used in large, complex institutions significantly reduce the risk of this type of event. Unexplained or inadequately explained anomalies should prompt a production rerun. Event report logs for unexplained anomalies should be forwarded to the **computer incident response team** for review.

Page 35: Management should train and test operations personnel on their ability to recognize security events that require referral to the **computer security incident response team**, security guards, management, or other parties. Social engineering is a growing concern for all personnel, and in some organizations personnel may be easy targets for hackers trying to obtain information through trickery or deception.

Page 39: Much of IT operations can and should be subject to measurement based on the size and complexity of the institution. The information gained from analysis supports not only daily management of operations and early diagnostics on impending problems, but provides the baseline and trend data used in capacity planning.
Examples of operations performance metrics include the following:

- [Excerpt] Electronic funds transfer and electronic banking:
  -Number of wire processing errors caused by department and percent of total volume;
  -Number of wires not processed due to failure to execute; and
  -Number of **incidents** reported and compensation paid due to department processing errors.

SOURCE: FFIEC E-BANKING BOOKLET

Page 23: As with all outsourced financial services, institutions must have a formal contract with the TSP that clearly addresses the duties and responsibilities of the parties involved. In the past, some institutions have had informal security expectations for software vendors or Internet access providers that had never been committed to writing. This lack of clear responsibilities and consensus has lead to breakdowns in internal controls and allowed security incidents to occur. The IT Handbook's "Outsourcing Technology Services Booklet" lists detailed contract recommendations for TSPs. Institutions should tailor these recommendations to e-banking services as necessary. Specific examples of e-banking contract issues include

- [Excerpt] **Incident response plans**, including notification responsibilities, to **respond** to website outage, defacement, unauthorized access, or malicious code

Page 25: ***Security incidents***. Reports might include volume of rejected log-on attempts, password resets, attempted and successful penetration attempts, number and type of trapped viruses or other malicious code, and any physical security breaches.

Related Policies / Procedures / Tools

- Incident Response Program At-large
  - [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] Meeting Procedure
  - [Incident Response Team (IRT) / IRT / Technology Steering Committee / Disaster Recovery Team] Training Presentation
  - Incident Response Decision Tree
  - Incident Response Plan
  - Intrusion Detection Procedure
  - Potential Incident Report
  - Suspicious Activity Report (SAR)
  - Third Party Information Request Procedure
  - Virus Incident Response Procedure
  - Web Defacement Procedure
- Other Programs:
  - IT Governance Policy
  - Business Continuity Plan
  - Disaster Recovery Plan
  - Business Impact Analysis
  - Vendor Management Policy

Policy Owner

- Title Here

Policy Reviewers

- Board of Directors
- Incident Response Team
- [EDP / IT Steering / Technology] Committee
- Titles Here

Development History

List the dates that this documentation was changed, starting with the creation date at the bottom. For each modification, include effective date and policy owner.

- Modified: xx/xx/xx; policy owner
- Creation Date: xx/xx/xx: policy owner

Policy

Reading Time!

Incident Response Policy

infotex

Buzzword Notes

- We did not ñcyberò up our boilerplate.
- We didnôt ñmobileò up our portable device boilerplates in 2008 either.
- But we did change ELM to SIEM!

infotex

Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Framework
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

The Incident Response Plan

- Components of a Good Plan
- Reporting Requirements
- Training Considerations

Common to Bad Plans

- Does not address specific threat scenarios
- Does not have procedures for evaluating customer information exposure
- Forget to notify regulator and /or file a SAR
- No standard incident response documentation
- Nobody knows whatôs in it. (The plan is not tested.)

infotex

Birdôs Eye View

- Three primary elements:
  - Training
  - Process Guidelines
  - Reporting Requirements

infotex

High Level View

- Training
  - Definitions
  - Goals and Priorities
  - Incident Types (from policy)
  - Authority and Responsibilities
  - Shared Passwords
  - Technical Controls

infotex

High Level View

- Process Guidelines
  - Incident Management
  - Severity Ratings
  - Technical Controls
  - Social Media Monitoring Guidelines
  - Forensics

infotex

Reporting Requirements

- Incident Reporting
  - Disclosure Events
  - Severe Security and Negative Events
  - Summary Reporting
- Trend Reporting
  - IRT Meeting Reports
  - Annual Report to the Board

infotex

Incident Response Plan

- Establishes a broad-based interpretation of the term: ñIncident.ò
- Relies upon an understanding of the ñintrusion,ò how it works, and how it is detected.
- Establishes details of the reporting requirements.

infotex

Incident Response Plan

- Reiterates rules and procedures required by the board level policy.
- Establishes basic goals and priorities of Incident Response.
- Establishes the framework of an Incident Response Process.
- Establishes response guidelines.

infotex

Incident Response Plan

- Establishes:
  - An Incident Management Process
  - Impact Severity Rating Guidelines
  - Notification Requirements
  - Regular Reporting Requirements
- Maintains
  - Guidelines for Managing an MSSP
  - Critical Information Storage Guidelines

infotex

Incident Response Plan

- Creates:
  - A set of "suspicious activity triggers."
  - A process for reporting potential incidents by Information Technology Team Members (PIR).

infotex

Incident Response Plan

- Calls for:
  - Tools for training members of the IRT -
    - The plan itself
    - Meeting Procedure and Agenda
    - Testing Procedures (three documents)
    - Decision Tree, Notification Tools, etc.
  - Forms and templates to be used -
    - For Potential Incident Reports
    - For disclosure to customers
    - For engaging with the media

infotex

Framework of Response Process

- Overview - What are the goals and objectives in handling the incident?
- Evaluation - How serious is the incident? Assign a Severity Rating.
- Notification - Who should be notified about the incident?

infotex

Framework of Response Process

- Response - What should the response to the incident be?
- Legal/Investigative - What are the legal and prosecutorial implications of the incident?
- Documentation Logs - What records should be kept from before, during, and after the incident?

infotex

Metrics to Consider

- Time and Date of Incident
- Broadcast Awareness Time
- Time / Date of Containment

- # of Records
- Scope of breach (list of data fields)

infotex

Response Guidelines

- Containment
- Eradication
- Recovery
- Follow-up **(Postmortem or Post-Incident Analysis)**

infotex

Incident Management

- Who is responsible for
  - Classifying the incident (assigning a severity rating)?
  - Notifying Management and/or the IRT?
  - Calling a IRT meeting?
  - Determining physical and electronic evidence to be gathered and protected?

infotex

Incident Management

- Who is responsible for
  - Determining if company-wide communication is warranted?
  - Ensuring damage is repaired?
  - Communicating with third party system vendors and/or informing them of vulnerabilities?

infotex

Incident Management

- Who is responsible for
  - Initiating, documenting, and completing incident investigation?
  - Communicating with law enforcement?
  - Filing a SAR when necessary?

infotex

Shared Passwords

- There are a whole set of passwords that, unlike the network or application passwords, are known by more than one individual.
- Examples of these passwords include:
  - Firewall Passwords
  - Web Domain Name Registrars
  - Web Hosting administrator passwords
  - Router passwords
  - ñLocal Administrator Passwordsò
  - Stand-alone Application Passwords

infotex

Severity

- Even if you default to the more simplistic severity method, consider moving the browned language to a separate ñtoolò that you use to help determine severity.
- Remember: during a panic, anything already written will make your life easier.

infotex

Severity Questions

- Is there a possibility that we will need to notify our customers?
- Is this a multi-site incident?
- Are many computers at your site affected by this incident?
- Is sensitive information involved?

infotex

Severity Questions

- What is the entry point of the incident (network, phone line, local terminal, etc.)?
- Is the media involved?
- What is the potential damage of the incident?
- What is the estimated time to close out the incident?
- What resources could be required to handle the incident?

infotex

Severity Ratings

- Thresholds:
  - Often Coordinated with Disaster Recovery Plan
  - Based on three primary issues:
    - Length of service interruption
    - Malicious orchestrated attack
    - Disclosure of Nonpublic Customer Information

infotex

Notification vs. Regular Reporting

- Notification relates to an ongoing incident.
- Regular Reporting Characteristics:
  - Delivered at regular intervals to specific individuals or teams
  - Summary Reports
  - Trend Analysis
  - Ongoing Risk Analysis
  - Recommendations for Risk Mitigation

infotex

Notification Requirements

- Reporting to Management
- Board Notification
- Outreach Strategy
- Involving Law Enforcement
- Customer Notification

infotex

Regular Reporting Requirements

- Report Types
  - Service Availability Reports
  - Security Incident Reports
  - Detailed Follow-up Reports
- Report Recipients
  - What goes to CIRT
  - What goes from CIRT to Management
  - What goes to the Board of Directors
- When?

infotex

Are all incidents network-based?

- What about incidents that the IDS system will not see?
- How do members of the Information Technology Team report suspicious activity they witness?

infotex

Technical Controls

- Lists the systems in place to prevent or at least detect technical intrusions.
- Includes service level requirements for MSSP providers.

infotex

Incident Response Plan

- **Show 'em where to find things!**

infotex

Quick Scan

Reading Time!

Incident Response Plan

infotex

Boilerplate

Purpose

- This is a "template" Incident Response Plan to be used as a "starting point" for the sake of helping you develop your Incident Response Process.

Copyright / Permission to Use

- Permission to use this document is conditional upon you receiving this template directly from an **infotex** employee, **infotex** website or e-commerce site, or an **infotex** workshop / training presentation.
- By using this template either in its entirety or any portion thereof, you acknowledge that you agree to the terms of use as dictated in the "Transfer of Copyright Agreement" located at copyright.**infotex**.com. This agreement establishes that when you customize this template to your specific needs, your organization may have copyright of the customized document. However, **infotex** retains copyright to the template. This agreement also establishes that you will not share this or any other template with third parties other than auditors and examiners. You may not transfer ownership of the customized documents to any other organization without the express written permission of **infotex**.

Instructions

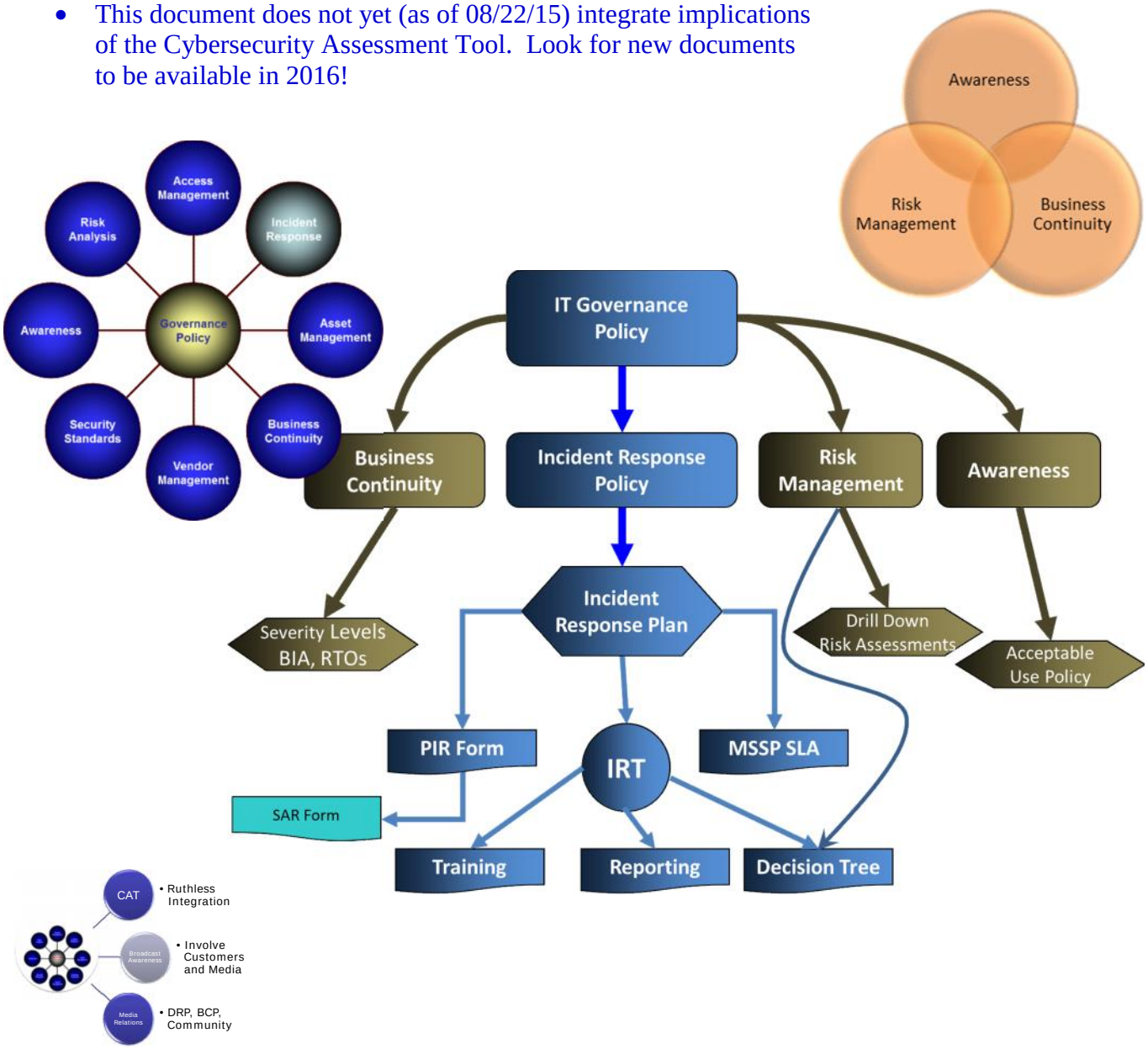
- Make sure to read through the template carefully as not all situations will pertain to your organization. However, to assist you in customizing the document to your specific needs, we have attempted to color code areas that will need your special attention. Color coding is as follows:
  - All areas needing customization and/or consideration are in **red**.
  - Sections that are in **brown** are optional sections according to our definition of best practices. These sections may be removed if they do not match your needs.
  - Sections in **blue** are merely instructions or additional information for knowledge purposes and should be removed.
  - Sections in **green** are examples.
- Note that you should confirm that all text has been changed to "black" before considering this template final for your organization. If there are any sections in any other color than black, then all situations or customization has not been considered.

This section (Templates) may be removed once the document has been customized, for at that time we turn ownership of the customized document over to you.

© Copyright 2000 - 2013 **infotex**, Inc. All rights reserved.

NOTES ABOUT THIS DOCUMENT:

- The incident response plan enforces the board-level Incident Response Policy, which sees Incident Response as the intersection of Awareness, Risk Management, and Business Continuity.
- This document should be used to train the IRT as well as a starting point during an incident. Usually incidents can cause a sense of urgency and often a state of paralysis. This plan should be pulled out to help center the team.
- This document does not yet (as of 08/22/15) integrate implications of the Cybersecurity Assessment Tool. Look for new documents to be available in 2016!



Insert Financial Institution Name / Logo

Incident Response Plan

(Approved During DD/MM/YY Incident Response Team Meeting)

Classified: Confidential Information

Contact if found: Name, Title

Name of Financial Institution

City, State

Plan Scope

This plan applies to all Name of Financial Institution's [Computer Incident Response Team (Computer Incident Response Team) / Incident Response Team (IRT) / Technology Steering Committee] as well as all members of the Information Technology Team. A portion of this plan, related to Suspicious Activity Reporting, pertains to each and every member of the Information Technology Team.

The [Computer Incident Response Team / IRT / Steering Committee], through the leadership of the Information Security Officer, is responsible for overseeing the development, implementation, and maintenance of this plan. It should be reviewed at least annually to ensure relevant information is appropriately considered.

The Information Security Officer is responsible for enforcing this plan.

For questions concerning this plan, see [the Information Security Officer / Senior Management].

Introduction

The Board of Directors has approved an Incident Response Policy which provides for the creation of a [Computer Incident Response Team / IRT / Steering Committee] and directing that team to be led by the Information Security Officer. The policy also requires the creation of this Incident Response Plan, including:

- An Intrusion Detection Procedure that establishes an Intrusion Detection System and parameters related to maintaining this system;
- An Incident Response Plan that serves as a guideline for an overall approach to incidents;
- Processes for containment, eradication, recovery, and follow-up;
- A procedure that includes a severity rating assignment process for incident types;
- Notification requirements establishing guidelines for reporting incidents;
- Regular reporting requirements for summary reports to Management and the Board of Directors;
- Provisions for documentation of critical information necessary in the event of an incident; and,
- Guidelines for IT personnel to report observed suspicious activity (with suspicious activity triggers).
- Priorities to serve as a starting point for defining responses to incidents;
- An Incident Management Procedure that includes a Severity Rating Assignment Process that breaks all incident types into five levels which will be used to dictate reporting requirements as well as require an emergency [Computer Incident Response Team / IRT / Steering Committee] meeting.

Objective

Given the risk-based approach to Information Security and that there is no such thing as 100% security, management must create a proactive plan for addressing incidents where availability of information, integrity of information, or confidentiality of information is breached. Likewise, the plan should ensure that the financial institution properly addresses violations of the Acceptable Use Policy. The plan should establish the goals of good incident response, as well as priorities to enforce while in an incident.

Accordingly, the Federal Financial Institutions Examination Council (FFIEC) indicates that the IT operations management should implement corrective (incident response) security controls.

The Incident Response Policy also creates the [Computer Incident Response Team / IRT / Steering Committee] , establishing the membership, roles, responsibilities, and authority of the [Computer Incident Response Team / IRT / Steering Committee] . Note: Most banks are now calling this team the "Incident Response Team" because this policy governs more than just computer incidents.

Though for the purposes of creating an incident response process we will not include these types in our classification structures, it is helpful to know that the following types of negative actions can be considered to be a "technology incident."

- Increased Access
- Disclosure of Information
- Corruption of Information
- Denial of Service
- Theft of resources
- Negative Reputation
- Negative Legal Implications

For the sake of this plan, an "incident" is anything that occurs that negatively impacts upon the institution, its employees, or its customers. This includes incidents related to [availability,] integrity, confidentiality, legal risk, and/or reputational risk. Incidents related to availability will be addressed by the Business Continuity Plan as per the Business Continuity Policy.

High Likelihood Response Scenarios

A secondary objective of this Incident Response Plan is to, with the assistance of the Incident Response Team, proactively develop incident response scenarios with plans surrounding those scenarios for the high-likelihood incidents as determined by our risk assessment process. Scenarios will be tested as per FFIEC Guidelines related to Disaster Recovery Testing. See Appendix B for these test scenarios.

Goals of an Incident Response

The main goals of a response to an incident are as follows:

- Proactive Goals
  - Assure integrity of critical information assets.
  - Detect intrusion, misuse, and other negative events.
  - Recover systems, data, and services.
  - Contain intrusions and negative incidents.
  -
- Reactive Goals
  - Investigate the source or cause of an incident.
  - Facilitate and control communication with internal and external agencies.
  - Investigate in a manner that will allow prosecution where appropriate.
  - Feed the Suspicious Activity Reporting procedure.

- Reactive Proactive Goals
  - Allow for trend analysis, on-going risk assessment, and mitigation.
  - Educate the [Computer Incident Response Team / IRT / Steering Committee].
  - Heighten awareness of appropriate team members.
  - Consider the type of incidents that could occur

Priorities

The following priorities serve as a starting point for defining our organization's response:

1. Protect human life and safety.
2. Protect customer information and assure organizational data integrity.
3. Maintain the financial institution’s reputation and control external communication.
4. Prevent damage to systems.
5. Minimize disruption of computing resources.

Types of Incidents

The [Computer Incident Response Team / IRT / Steering Committee] will classify all incidents into one of three types:

- Disclosure Incidents: These are incidents which, because of some statute or regulation, require [name of financial institution] to notify customers, law enforcement, examiners, or the board of directors. The [Computer Incident Response Team / IRT / Steering Committee] must comply with all applicable laws and regulations, including state laws such as [Indiana Code 24-9.4 / applicable law in your state] and the FFIEC's Financial Institution Letter 27-2005.
- Security Incidents: These are incidents related to the confidentiality and integrity of information. They can include technical incidents such as malware (virus, worm, and trojan horse) detection, unauthorized use of computer accounts and computer systems, but can also include non-technical incidents such as improper use of information assets as outlined in the Acceptable Use Policy.
- Negative Incidents: These are incidents related to the availability of information assets or other risks such as legal risks, strategic risks, or reputational risks that do not directly impact the confidentiality or integrity of information. For example, installing an unlicensed application on a bank-owned application does not impact confidentiality, integrity, or availability, but this policy still requires the [Computer Incident Response Team / IRT / Steering Committee] to track it.

The [Computer Incident Response Team / IRT / Steering Committee] may develop a severity classification system within each incident type. The Information Security Officer to report all Notification Incidents to the Board of Directors as they occur, and report [severe / critical] Security Incidents and [critical / severe] Negative Incidents as deemed necessary by the [Computer Incident Response Team / IRT / Steering Committee] in real time.

The Information Security Officer is authorized by the Incident Response Policy to classify incident types, as defined above, as well as incident severities. All incidents should be summarized by type and [criticality / severity] (as described below) in the Annual Report to the Board. This report should include status information for all "disclosure incidents."

Authority

The Information Security Officer is authorized by the Incident Response Policy to declare incident categories as described above, as well as incident severities as described below, even if the [Computer Incident Response Team / IRT / Steering Committee] does not agree with such classification. The Information Security Officer is responsible for coordinating and training the [Computer Incident Response Team / IRT / Steering Committee] related to Incident Response duties. The Information Security Officer is responsible for documenting and reporting incidents as well as overseeing the proper execution of the incident response procedures. This includes reporting incidents to the Board of Directors, Management, the [Computer Incident Response Team / IRT / Steering Committee], regulatory agencies, and law enforcement personnel, as appropriate.

It is the responsibility of all staff to adhere to all Name of Financial Institution security policies and procedures, and promptly report information security incidents as defined in this policy. All Managers of the Information Technology staff are responsible for ensuring that incident reporting policy and procedures are communicated to and understood by all staff under their authority. The [Network Manager / Network Administrator] is responsible for immediately reporting all incidents, including

unexplained system downtime, drastic changes in system performance, suspicious probes and browsing, and/or denials of service to the Information Security Officer. Detailed documentation describing the incident must also be submitted.

Only the following people have the responsibility and authority to define, set, and change firewall rulesets and routing controls; change or authorize change of IDS signatures; as well as affect any other device or software that has or may have an impact on the security of the network:

- IT Manager / Network Administrator
- Chief Information Officer
- Network Provider
- Managed Security Services Provider

Responsibilities

- The Information Security Officer is responsible for classifying the incident as [a critical incident / one potentially requiring immediate action] (and thus an emergency meeting of the [Computer Incident Response Team / IRT / Steering Committee] or a [minor / trend] incident requiring review in a [monthly / quarterly / periodic] [Computer Incident Response Team / IRT / Steering Committee] meeting.
- The Information Security Officer, working with the [Computer Incident Response Team / IRT / Steering Committee], will what type of communication is required, the content of the communication, who should receive the communication, and how best to distribute the communication.
- The Information Security Officer is responsible for initiating, completing, and documenting the incident investigation with assistance from the [Computer Incident Response Team / IRT / Steering Committee].
- The Information Security Officer is responsible for managing and collecting forensic evidence, and will act as the contact person between the financial institution and law enforcement.
- The [Public Relations Officer / President / Marketing Director] is responsible for coordinating communications with outside organizations.
- In the event of internal policy violations, the Human Resources Department will recommend disciplinary actions, if appropriate, to the [Computer Incident Response Team / IRT / Steering Committee].

Incident Response Tests

The Information Security Officer will plan for and coordinate testing of the Incident Response Program. These tests should be conducted on an annual basis at least twice, and one of the tests should be of a scenario which would be classified as a "Disclosure Incident." All Incident Response Team members should attend the tests. Tests should include a test plan, minutes of the actual test, and documentation of a "post-mortem review." Test results should be presented to the board. A walk-through test should be conducted when the plan is updated. A tabletop test should be conducted against a high likelihood "incident scenario." Functional tests, conducted during social engineering portions of audits or internally, should also be conducted.

Broadcast Awareness

The Information Security Officer will create, publish, and maintain a process for quickly moving through "triage" on new incidents. This process will be named "Broadcast Awareness," and should be addressed in the Acceptable Use Policy as well as in annual awareness training. Whenever possible, the time to broadcast awareness should be measured in tests and incidents. The Information Security Officer should work with auditors to determine broadcast awareness time during social engineering steps as well as block time on IPS systems. Broadcast Awareness should be determined, when possible, as a metric during a live incident. The process should articulate what happens from the time an employee becomes suspicious until when we notify the media (see diagram to left.)

First Priority in an Incident

The incident response team will be trained that the first priority in an incident is to contain the incident . . . stop any further damage from being incurred. All users will be taught a "last resort response . . . . go into 'airplane mode'" during suspected incidents.

Incident Response Team Steps

For those not involved in "containing" an incident, the first three steps in an incident should be to 1) Broadcast Awareness, 2) Inform the Information Security Officer, and 3) assist in the Triage process.

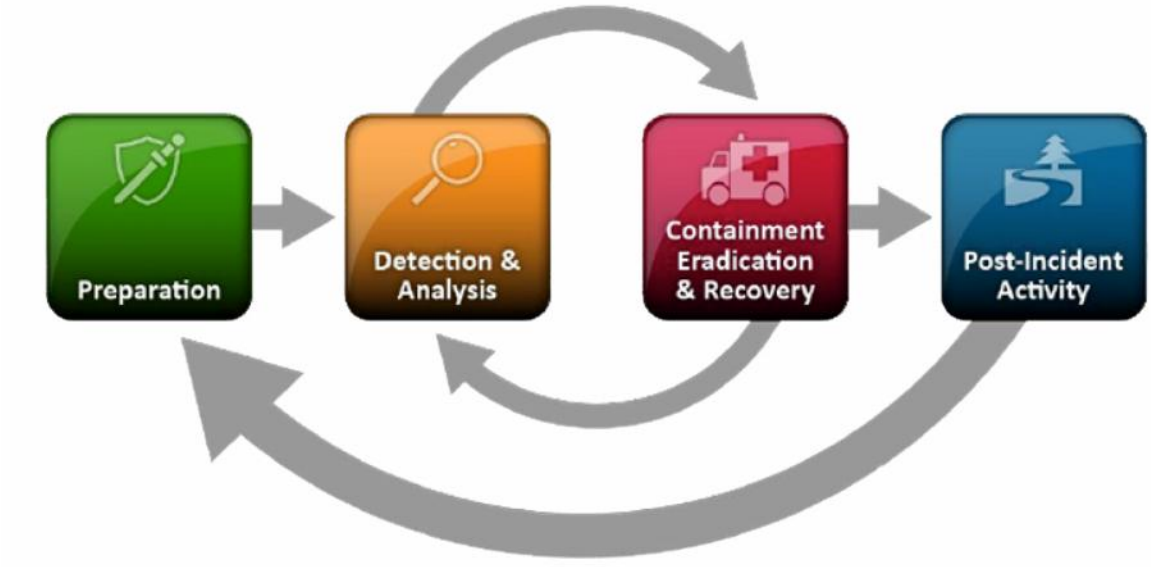
Triage

Triage is the name of our process for determining the scope and nature of an incident, resulting in the classification, documentation, and escalation (if necessary) of the incident in a timely manner. The three-step process is as follows:

1. Detect: Broadcast Awareness
2. Assess: Real or potential unauthorized access to customer data? Who, what, when, how, where?
    A. Has misuse occurred?
    B. Or is there a potential that misuse could occur?
3. Respond: Classify, Document, Escalate!

Response Cycle

The Incident Response Team will be trained on the NIST Response Cycle as indicated in the following drawing:



When Customer Notice is required

Guidance maintains that <Name of Financial Institution> must notify customers whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur.

Notification Tactics

Customer notice should be given in a clear and conspicuous manner. The notice should include the following items:

- Description of the incident;
- Type of information subject to unauthorized access;
- Measures taken by the institution to protect customers from further unauthorized access;
- Telephone number customers can call for information and assistance; and
- Remind customers to remain vigilant over next twelve to twenty four months, and report suspected identity theft incidents to the institution.

The guidance encourages financial institutions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of customers that include contact information for the reporting agencies.

Delivery of Customer Notice

Customer notice should be delivered in a manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

Compliance steps to Following during a Disclosure Incident

Guidance maintains that the following steps be followed in an Incident Response:

1. Triage: Assess nature and scope of incident and determine if customer notification is required. (Determine Disclosure Requirements)
2. Notify your federal regulator.
3. File a timely SAR.
4. Contain and Control
5. Notify Customer

We will of course contain an incident as a first priority. The above identifies the compliance steps that must be followed in an incident.

Risk Monitoring

The Information Security Officer will ensure that the Incident Response Team is monitoring accepted risk. When the Board of Directors accepts the risk on various information assets, this acceptance is based upon the understanding that the Incident Response Team is monitoring for a threat exploiting a vulnerability for known accepted risks. The Incident Response Team will be responsible for monitoring non-technical risk. The Information Security Officer may outsource, with Board approval, the monitoring of some technical risk. The Board of Directors requires that the Incident Response Team adopt [the NIST CyberSecurity Framework | NIST SP 800-61 | the FFIEC Guidelines] as the framework for which Risk Monitoring will be audited against. The Information Security Officer will inventory and/or diagram layers of risk monitoring controls.

Intrusion Detection Procedure

- Our intrusion detection is outsourced to a Managed Security Service Provider (MSSP). We have on file an agreement that the Intrusion Detection System (IDS) will be monitored 24x7x365. This agreement also provides for an 8 hour guaranteed response to any and all detectable intrusions.
- All financial institution employees will be trained to "broadcast awareness," meaning inform all appropriate persons in real time of suspicious activities. Then, all suspected and/or confirmed instances of attempted and/or successful intrusions must be immediately reported to the Information Security Officer.
- Information Technology Team Members will be trained by the Information Security Officer how to report potential issues they may discover as they troubleshoot and maintain the system, to the [Computer Incident Response Team / IRT / Steering Committee] for investigation.
- All incidents will be carefully assessed by the Information Security Officer to determine appropriate action and ensure necessary reporting requirements are met. Reporting based on system availability and customer information breach is described below. Still, not all incidents are easily predicted in terms of reporting requirements, and the Information Security Officer will need to make judgment calls based on the situation. As a general rule, reporting to the [Computer Incident Response Team / IRT / Steering Committee] will be required if the incident expands into an official investigation or there is a need to counsel an individual through Human Resources.
- Based on the nature and scope of the incident, technical staff and the Information Security Officer shall decide whether the incident can be resolved locally or whether additional assistance is required from the [Computer Incident Response Team / IRT / Steering Committee] or other outside sources.
- Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.

Incident Response Questions

At the Information Security Officer's discretion, based on the type of incident, the overall approach to an incident may be determined after answering questions as follows:

1. Overview - What are the goals and objectives in handling the incident?
2. Evaluation and Classification - How serious is the incident? Assign a Severity Rating.
3. Notification - Who should be notified about the incident?
4. Response - What should the response to the incident be?
5. Legal/Investigation - What are the legal and prosecutorial implications of the incident?
6. Documentation Logs - What records should be kept from before, during, and after the incident?

Response Guidelines

At the Information Security Officer's discretion, based on the type of incident, the actual response to an event may fall into the general categories of containment, eradication, recovery, and follow-up. Response usually occurs concurrently with overview, evaluation, and notification. Timely response is, of course, one of the keys to mitigating damage.

A. Containment: The purpose of containment is to limit the extent of an attack. For example, it is important to limit the spread of a worm attack on a network as quickly as possible. An Incident Response Decision Tree is on file at our managed security service provider's NOC, where predetermined containment procedures have already been addressed. An essential part of containment is assigning a severity rating to the incident as well as decision making (i.e., determining whether to shut a system down, to disconnect from a network, to monitor a system or network activity, to set traps, to disable functions such as remote file transfer on a UNIX system). Notification occurs during this stage.

B. Eradication: Once the incident has been contained, it is now time to eradicate the cause. Eradication software is available to eliminate most viruses that infect small systems. Ensure all backups are clean. Many systems infected with viruses become re-infected periodically because people do not systematically eradicate the virus from backups.

C. Recovery: The goal of recovery is to return the system to normal. In the case of a network-based attack, it is important to install patches for any operating system vulnerability which was exploited. All compromised systems are to be restored before reactivation.

D. Follow-up: Follow-up should include regular status reporting, describing new controls and "lessons learned" to improve future performance.

The most important element of the follow-up stage is performing a postmortem analysis of the response procedure itself. Exactly what happened and at what times? How well did the staff involved with the incident perform? What kind of information did the staff need quickly, and how could they have received that information as soon as possible? What would the staff do differently next time? Creating a formal chronology of events (including time stamps) is also important for legal reasons. Similarly, it is important to quickly obtain a monetary estimate of the amount of damage the incident caused in terms of any loss of software and files, hardware damage, and manpower costs to restore altered files, reconfigure affected systems, and so forth. This estimate may become the basis for subsequent prosecution activity.

Forensic Investigation

When an incident is a result of a computer crime or has the potential of being part of a legal proceeding, evidence can be derived from computers and then used in court against suspected individuals. Computer evidence is like any other evidence; it must be authentic, accurate, complete, convincing to juries, and in conformity with common law and legislative rules. Thus, the evidence gathered from suspected computer-related crimes must conform to the same standards as other evidence to be credible.

The Information Security Officer is responsible for managing the collection of forensic evidence. The IT Manager and Information Security Officer will proactively establish standards and rules related to forensics evidence collection. (Note: use last sentence if the following is not used.) The following rules will be followed:

- Ensure that no forensics evidence is damaged, destroyed or otherwise compromised by the procedures used during the investigation.
- Never work on the original evidence.
- Establish and maintain a continuing chain of custody.
- Document everything.
- Consider hiring a third party to collect evidence in a forensics-proof manner. The independence of a third party will increase credibility of evidence, and the appropriate vendor will be trained to identify, acquire, and preserve evidence in the proper manner, as well as keep a proper chain of custody.
- The Information Security Officer has the authority to hire and/or retain a third party to collect Forensics data so that independence is established and there is no appearance of a conflict of interest.

Severity Rating Assignment

Some organizations will assign a "disaster/availability" criticality to appropriate incidents and continue to track, monitor, and report on it in the Incident Response Program. However, other banks will only use two severity ratings (Minor and Critical, for example) and refer all availability related incidents, even if created by viruses or other denial-of-service attack vectors, to the disaster recovery component of the business continuity plan, and track, monitor, and report on it from there.

To simplify the response process, the Information Security Officer will assign one of [three / two] severity ratings to incidents as they are reported.

1) [Minor / Trend] Incident: This incident is low risk and, though [may/should] be monitored and reported in an upcoming [Computer Incident Response Team / IRT / Steering Committee] meeting, does not warrant immediate action or reporting.
2) [Critical / Severe / Emergency] Incident: This incident requires an emergency [Computer Incident Response Team / Incident Response Team / Steering Committee] Meeting to determine response actions, notification requirements, etc.

Note: Some banks do not specify disaster incidents as a third incident, and just have the second paragraph below.

3) Disaster (Availability) Incidents: This incident requires execution of the Disaster Recovery Plan, and will defer to response processes and severity ratings in that plan. . . . or . . .

Disaster Incidents: Some incidents require execution of the Business Continuity Plan, and will defer to response processes and severity ratings in that plan, as decided by the Information Security Officer.

Or, for larger organizations, the following may be used in place of the above simplified severity classification scheme:

In order to identify the scope and impact, a set of criteria should be defined which is appropriate to the site and to the type of connections available. Critical questions must be asked to help determine the severity of the incident.

- Is there a possibility the a possibility that we will need to notify our customers?
- Is this a multi-site incident?
- Are many computers at your site affected by this incident?
- Is sensitive information involved?
- What is the entry point of the incident (network, phone line, local terminal, etc.)?
- Is the media involved?
- What is the potential damage of the incident?
- What is the estimated time to close out the incident?
- What resources could be required to handle the incident?

Note: Even smaller institutions, if not including the above in their actual plan, may want to have a separate "tool or standards" document with the above questions to assist in an incident.

In order to ensure a response process that assures prompt notification of senior management and the board as dictated by the probable severity of damage and potential monetary loss related to adverse events, the Information Security Officer must review all incident reports to sort between the following levels of severity:

Level 1) Minor Incident

No interruption in data processing operations.

All incidents that will not affect operation of business but need to reported to Management/[Computer Incident Response Team / IRT / Steering Committee] in monthly written reports.

Level 2) Reportable Incident

Some computer facility and/or computer equipment damage or an interruption in critical services is observed, but operations can be resumed within 12 hours. Note: equalize this time-frame to the financial institution's Disaster Recovery Plan. Any incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of 12 hours or less.

OR Any security incident which has been successfully responded to and which does not have the potential, over time, to affect inherent operational or reputational risk.

Level 3) Major Incident:

Moderate damage to the computer facility and/or the computer equipment or an interruption in critical services is observed, but operations can be resumed within 12 to 40 hours. Note: equalize this to the financial institution's Disaster Recovery Plan. User departments would experience two or less working days delay of updated information. Any incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of more than 12 to 40 hours.

OR Any security incident which it is clear that a person has been specifically targeting the financial institution for the purpose of breaching security.

Level 4) Critical Incident:

Any incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of more than 12 to 48 hours. Note: equalize this to the financial institution's Disaster Recovery Plan.

AND/OR Any security incident which it is clear that a person has breached security of the financial institution or for some other reason the Information Security Officer determines that the [Computer Incident Response Team / IRT / Steering Committee] may want to consider involving law enforcement.

AND/OR Any event that may increase reputational or legal risk if not addressed immediately.

AND/OR Any security incident in which protected customer information has been breached.

Level 5) Disaster:

Any Level 3 incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of more than 48 hours. Note: equalize this to the financial institution's Disaster Recovery Plan.

Critical Information Storage

A Managed Security Service Provider will be required to host an offsite, secure "information safe" in which the following will be stored and kept current:

- Corporate Disaster Recovery Plan
- Shared Passwords
- Network Diagram
- Organizational Calling Tree and Distribution List

Risk Monitoring and Preventive Controls

Note: List the types of detective, preventive, and monitoring controls the Organization uses for cybersecurity incidents.

The Network Administrator is responsible for maintaining the following automated systems, which are in place to prevent an incident:

- **Virus Prevention:** Name of Financial Institution uses [name of virus protection package] to detect, quarantine, and remove viruses. The package is installed on the [name of server] and feeds DATS to all workstations [hourly / daily / weekly / as-needed]. Workstations are audited [quarterly / semi-annually] as well as randomly to establish that DATs are current. See the Virus Incident Response Procedure for more details.

- **Spam Filtering:** Name of Financial Institution uses a multi-layered spam defense approach, starting with [name of spam filter] which is a[n] [server-based / network device / off-site] spam filter. False positives go to [individual user / supervisor / departmental / central] quarantines and users [log in to / request reviews of / can directly review] the quarantine to review the quarantine to release legitimate messages. Users can also identify spam (delivered messages that should have been filtered). The system learns from such activity. The [Offsite Filtering / Spam Filtering] system also filters viruses, adding an additional layer of protection to our existing virus protection strategy.

- **Content Filtering:** Name of Financial Institution uses [name of content filter] which blocks requests for certain URL's that are considered inappropriate. Users that need temporary access to certain web pages that may request an exception to the content filtering policy. The [Network Administrator] approves such exceptions. Policies are established based on the [Network Administrator]'s interpretation of the Acceptable Use Policy. Lexicons related to sites that expose Name of Financial Institution to legal risk, such as pornographic, illegal, hate-based, and other offensive websites are turned on. Other lexicons which are turned on include [e-commerce sites such as e-bay, chat room sites, list sites here].

- **Spyware Screening:** Name of Financial Institution uses [name of spyware screening software] to block spyware at the perimeter of the network. The Intrusion Detection System [also] functions in this capacity.

- **Intrusion Prevention System:** Name of Financial Institution uses [name of IPS/IDS system] to monitor all network traffic. The preventive functionality of this system works in a "blocking mode," meaning that it provides a preventative control by automatically blocking certain incident types, such as spyware, vulnerability scans, etc.

- **Intrusion Detection System:** Name of Financial Institution uses [name of IPS/IDS system] to monitor all perimeter and internal network traffic that cannot be blocked with an Intrusion Prevention System. This system creates a detective control,, and Name of Financial Institution outsources the monitoring of this system so that incidents can be responded to in real time.

- **Event Log Management System (SIEM):** Name of Financial Institution uses [name of IPS/IDS system] to monitor all critical logs generated by critical information assets. Correlation of logs to network traffic is handled by [name of IPS/IDS provider.] Log analysis definitions are kept by the Information Security Officer. (Note, some MSSPs won't share this information.)

- **File Integrity Checking Processes:** Name of Financial Institution has the following "change detection" processes in place: Web Defacement Monitoring provided by [name of company.] Change Detection (of port modifications) on the firewall using [name of system.] File integrity checks on the firewall rules file using [name of system.] Describe other file integrity checking processes in place.

- **Social Media Monitoring:** Name of Financial Institution uses processes defined below to monitor the internet for the bank's name and derivatives of the bank's name. In the event a negative comment is published about the bank, appropriate persons are notified according to the decision tree.

- **Other Third Party Monitoring:** Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams. Document any arrangements you have made here.

- **Incident Response Team:** We use our Incident Response Team to monitor for threats exploiting vulnerabilities in a manner that cannot be detected by technical controls. For example, the world's greatest is not going to detect a pretext call. Thus, the following roles have been assigned:
    - Human Resources: Monitors for policy violations, internal threats, employees in financial trouble, and security awareness issues.
    - Marketing: Monitors for media threats, inappropriate social media posts, customer awareness issues. Also prepares for customer notification and media engagement.
    - Identify a Person: Monitors FS-ISAC.
    - Identify a Person: Engages with law enforcement and brings any news to the Incident Response Team meetings.
    - Identify a Person: Engages with the [State Banking Association]
    - Identify a Person: Engages with [Infragard, Cert, Local Organizations, etc.]

Managed Security Provider Response Procedures

Note: The following procedure is based on the infotex Controlled Response IPS system . . . you will need to tailor this to your own MSSP.

- The procedures for initial response and containment for all incidents by type are documented in the Incident Response Decision Tree.
- The procedures for notification of incidents as they occur are documented in the Communication Methodology of the Managed Security Service Provider's portal.
- Necessary passwords for response to incidents in real time are secured offsite in the Information Safe.
- Some Incident Response Procedures place the containment and eradication back in the hands of our IT staff. In general, these are usually virus incidents, compromised website incidents, and some network incidents.
- Specific Procedures for response to Virus Incidents, Compromised Website Incident, and Network Incidents are addressed in separate documents (see supporting information below).
- Almost always the follow-up phase of intrusion response is handled by the [Computer Incident Response Team / IRT / Steering Committee] as per the Policy Rules in the Incident Response Policy.

Managed Security Service Provider Requirements

The MSSP is required to:

1. Utilize CISSP personnel to design, manage, and oversee the [SOC / NOC];
2. Conduct background checks on all NOC personnel;
3. Submit financial statements for review annually;
4. Maintain a nondisclosure agreement;
5. Maintain a provable chain of custody for the preservation of potential evidence through such mechanisms as a detailed action and decision log indicating who made each entry.

In addition to the normal vendor management responsibilities, a successful engagement with an MSSP should include:

- A contract with mutually agreed upon Service Level Agreements (SLAs);
- Strategies for ensuring transparency and accountability that include:
- Regular communication between the FI and the MSSP on
- matters including change control, problem resolution,
- threat assessments, and MIS reporting,
- Descriptions of processes for physical and logical controls over bank data; and,
- Periodic review of the MSSP's processes, infrastructure, and control environment through offsite reviews of documentation and onsite visitations.

See FFIEC Guidelines for managing an MSSP (Appendix D of the IT Examination Handbook).

Furthermore, the MSSP must provide third-party assurance that the following is in place:

- Adequate controls used to detect and respond to unauthorized activities;
- Schematics of the information technology systems for common intrusion detection systems;
- Assurance that an appropriate firewall ruleset and routing controls are in place and updated as needs warrant;
- Assurance that appropriate filtering occurs for spoofed addresses, both within the network and at external connections, covering network entry and exit;
- Assures that logs of security related events are sufficient to assign accountability for intrusion detection system activities, as well as support intrusion forensics and IDS;
- Appropriately secures logs of security related events against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected;
- Has in place an appropriate process exists to authorize employee access to intrusion detection systems and that authentication and authorization controls limit access to and control the access of authorized individuals.

Managed Security Service Provider (MSSP) Service Level Agreement (SLA):

The following is a summary of the Service Level Agreement with the MSSP:

- Start Date: xx/xx/xx
- Expiration Date: xx/xx/xx
- Renewal Terms: Month to Month
- Guaranteed Response Time: x Hours
- Intrusion Prevention on the Network Perimeter: Yes
- Intrusion Detection on the Network Perimeter: Yes
- Intrusion Prevention on the Internal Network: Yes
- Intrusion Detection on the Internal Network: Yes
- Real-time monitoring of critical event logs: Yes
  - Definition of Critical Logs: As per below
- Collection and Forensics Archival of Logs: As per below
- Ability to provide trend reports to IRT Meetings: IPS/IDS only
- Change control on the firewall.
- Web Defacement Monitoring
- List other services here . . .

Definition of Critical Logs

By default: the following log events are monitored as the system is polled (every 15 minutes) and, when occurring, triggers an immediate reaction via the Infotex 24x7x365 Network Operations Center team:

- Disk Capacity Failures
- Unexpected Server reboots
- Windows Update Failures
- Licensing Errors
- Hardware Errors (as requested by Client during tuning)
- Backup Errors (as customized to Client during tuning)
- DNS Errors (as requested by Client during tuning)

Collection, Consolidation, and Forensics Archival of Logs:

- Account Management – Success / Failure
- System Events – Success / Failure
- Directory Service Access – Success / Failure
  - Active Directory Object Access Attempts – Success / Failure
  - Active Directory Object Deletions
  - Group Policy Management
  - User account changes that provide administrator equivalent permissions.
  - Changes to Groups --- adds, changes, or deletions. .
- Password Reset Attempts by Users
- Password Reset Attempts by Administrators or Account Operations
- Login Events – Success / Failure
- Disk Capacity Failures
- Manual changes to the registry – adds, changes, and deletions.
- AVS Application Update errors (as customized by Client during tuning)
- AVS DAT Update Errors (as customized by Client during tuning)
- Unexpected Server reboots
- Access to Network Infrastructure
- Changes to ACL's on switches, routers, or firewalls (assuming client includes these
- assets)
- Windows Update Failures
- Licensing Errors
- Hardware Errors (as requested by Client during tuning)
- Backup Errors (as customized to Client during tuning)
- DNS Errors (as requested by Client during tuning)

Notification Requirements

External communications to customers, law enforcement and/or the media must be reviewed by the [Computer Incident Response Team / IRT / Steering Committee], and presented to Management for approval prior to releasing it to the public. Specifically:

Customer Notification (Disclosure Incidents): [Indiana Law (Indiana Code section 24-4.9) / Applicable Local Laws] and FIL-27-2005 requires notification of customers in the event a breach of security jeopardizes non-public customer financial information. Specifically, FIL-27-2005 requires a five step process to be completed in order to respond to Disclosure Incidents:

1. Assess the nature and scope of the incident and identify what customer information systems and types of customer information have been accessed or misused;
2. Notify your primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
3. File a timely SAR, and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notify appropriate law enforcement authorities;
4. Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and
5. Notify customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it.

Furthermore, FIL-27-2005 defines customer information as:

- A customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account.
- The FFIEC's definition also includes any combination of components of customer information that would allow someone to log on to or access the customer's account, such as user name and password or password and account number.

Finally, FIL-27-2005 clarifies the timeframe we must follow for determining WHEN a customer is notified as follows:

- A financial institution should provide a notice to its customers whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur.

In this type of incident, the [Computer Incident Response Team / IRT / Steering Committee] will determine if legal counsel must be involved. Notification should include the date of the breach and the types of information that was breached. Notification should be reviewed by the PR / Marketing member of the [Computer Incident Response Team / IRT / Steering Committee] prior to delivery. The Board of Directors must be notified in the event of a Disclosure Incident.

Law Enforcement Notification: Law Enforcement will be notified if the incident warrants a criminal investigation. This includes, but is not limited to, theft of computer equipment or software, destruction of or tampering with government equipment, illegal Internet activity, electronic mail that poses a threat

to customers or staff and falsifying or stealing information contained in company systems. Investigative procedures will be followed to determine if criminal activity occurred. Pending preliminary investigation results, the Director of Security will work with law enforcement to meet further reporting requirements. The [Computer Incident Response Team / IRT / Steering Committee] and Management will be kept informed of the progress of the investigation as changes in the status of the investigation occur.

If law enforcement must be notified and an investigation initiated, a Suspicious Activity Report (SAR) must be filed with the Financial Crimes Enforcement Network (FinCEN). It is up to the [Computer Incident Response Team / IRT / Steering Committee] 's discretion as to whether incidents warrant the involvement of Law Enforcement and/or submission of a SAR to FinCEN. Note however, that Bank Secrecy Act regulations require every financial institution to file a report of any suspicious transaction relevant to a possible violation of law or regulation.

Board of Directors: The Board of Directors will be informed, in real time, of any incidents which require notification of customers, law enforcement, or other government agencies. Non-critical disclosure incidents still require board notification, but it can be part of a monthly report to the board. The Board of Directors will also receive a summary of incidents annually in the Annual Information Security Report to the Board.

One of the most important issues to consider is when, who, and how much to release to the general public through the media. There are many issues to consider when deciding this issue. First and foremost, if a public relations office exists for the financial institution, it is important to use this office as a liaison to the media. The public relations office is trained in the type and wording of information released and will help to assure that image is protected during and after the incident (if possible). Involving the public relations office in the [Computer Incident Response Team / IRT / Steering Committee] substantially reduces reputational risk. A public relations office has the advantage to communicate candidly with Point of Contact (POC) and then act as a buffer to the media so that control over the incident is maintained.

If a public relations officer is not available, the information released to the media must be carefully considered. If the information is sensitive, it may be advantageous to provide only minimal or overview information to the media. It is quite possible that the perpetrator of the incident will quickly review any information provided to the media.

While it is difficult to determine in advance what level of detail to provide to the media, some guidelines to keep in mind:

- Keep the technical level of detail low. Detailed information about the incident may provide enough information for copycat events or even damage the company's ability to prosecute once the event is over.
- Keep speculation out of media statements. Speculation of whom is causing the incident or the motives are very likely to be in error and may cause an inflamed view of the incident.
- When necessary, the Information Secuirty Officer will work with law enforcement professionals and/or third-party forensics experts to assure that evidence is protected. If prosecution is involved, assure that the evidence collected is not divulged to the media.
- Try not to be forced into a media interview before you are prepared. The popular media is

famous for the "2 a.m." interview, where the hope is to catch the interviewee off guard and obtain information otherwise not available.

- Do not allow the media attention to detract from the handling of the event. Always remember that the successful closure of an incident is of primary importance.

When the incident is closed, the [Computer Incident Response Team / IRT / Steering Committee] (or a designated party) will report the following:

- a description of the incident;
- the response process;
- the notification process;
- the actions taken to prevent further breaches of security.

Furthermore, a Suspicious Activity Report may be filed, at the BSA Officer's discretion with the appropriate authorities.

Consider using this for larger organizations:
Upon assigning the Severity Level, the Information Security Officer in coordination with the [Computer Incident Response Team / IRT / Steering Committee] must then implement proper reporting as follows:

Reporting to Management: Any Severity Level 5 incident (disaster) will immediately trigger execution of the financial institution's Disaster Recovery Plan. Levels 3 and 4 will require an immediate meeting of the [Computer Incident Response Team / IRT / Steering Committee] and Management will be informed immediately. Level 2 incidents will require a report to the [Computer Incident Response Team / IRT / Steering Committee] and further review in the next regularly scheduled [Computer Incident Response Team / IRT / Steering Committee] meeting. Level 1 incidents will be included in monthly reports to the [Computer Incident Response Team / IRT / Steering Committee] and Management.

Outreach Strategy: For Severity Levels 4 and 5 a press release must be drafted, reviewed by the [Computer Incident Response Team / IRT / Steering Committee] , and presented to Management for approval prior to releasing it to the press. The purpose of the press release is to mitigate damage to the financial institution's reputation. Accomplish this by assuring that depositor's money is safe and that security arrangements are being made. In the event of a breach of protected customer information assure the media that forensics are being arranged and the extent of the problem determined, and that all affected customers will be informed once the true nature of the damages are known. Refer to the financial institution's Business Continuity Plan for more information related to dealing with the media.

Information Sharing Procedures: In the event of incidents at Levels 3 or 4, documentation of the breaches must be shared in compliance with the financial institution's business continuity plan:

Either insert the Public Relations guideline from the Business Continuity Plan [which should list regulatory bodies, media contacts, etc.] into this point, or include the following reference: See Business Continuity Plan Section [identify section.]

Law Enforcement Notification: For Severity Level 3, 4 and 5 incidents, law enforcement must be notified and an investigation initiated. A Suspicious Activity Report (SAR) must be filed with the

Financial Crimes Enforcement Network (FinCEN). IDS forensics must be initiated. Security Vendors must be contacted to assist with documentation and forensics efforts.

The SAR should be filed with FinCEN no later than 30 calendar days after the date of initial detection by the institution of facts that may form the basis for filing a SAR. If no suspect was identified on the date of the detection of the incident requiring the filing, an institution may delay their filing for an additional 30 calendar days to identify a suspect. In no case can an institution delay filing a SAR by more than 60 days after the date of initial detection of a reportable transaction. Finally, if the situation requires immediate attention, the institution is expected to notify appropriate law enforcement by telephone in addition to filing a SAR. (See Appendix D for a blank Suspicious Activity Report form.)

It is up to the [Computer Incident Response Team / IRT / Steering Committee] 's discretion as to whether Level 2 incidents warrant the involvement of Law Enforcement and/or submission of a SAR to FinCEN. Note however, that Bank Secrecy Act regulations require every financial institution to file a report of any suspicious transaction relevant to a possible violation of law or regulation. Under the law, a SAR is triggered if the dollar amount involves at least $5,000 in funds or other assets and the institution knows, suspects or has reason to suspect that the transaction involves:

- Funds derived from illegal activity;
- Attempts to evade any requirements under the Bank Secrecy Act; or,
- No apparent business or lawful purpose or is not the sort of transaction in which the particular customer would normally be expected to be engaged in.

The Board of Directors must be notified when a SAR has been submitted.

Interface with Disaster Recovery/Business Continuity: In the event of a Severity Level 4 incident, the current IDS system vendor must be contacted as per Business Continuity Plan and arrangements for a replacement system made if determined necessary (alternative site in place more than X days or as determined by [Computer Incident Response Team / IRT / Steering Committee]).

- Point of Contact (POC) people (Technical, Administrative, Response Teams, Investigative, Legal, Vendors, Service providers), and which POCs are visible to whom.
- Wider community (users).
- Other sites that might be affected.

Regular Reporting Requirements

Monthly summary reports will be submitted to the [Computer Incident Response Team / IRT / Steering Committee] and then to Management.

Service Availability Reports: These reports will include statistics regarding the frequency and duration of service disruptions, including the reasons for any service disruptions (maintenance, equipment/network problems, security incidents, etc.); "up time" and "down time" percentages for website and e-banking services; and volume and type of website access problems reported by e-banking customers.

Security Incident Reports: These reports will include volume of rejected log-on attempts, password resets, attempted and successful penetration attempts, number and type of trapped viruses or other malicious code, and any physical security breaches. Critical severity incidents will be detailed in this report.

All severity levels 1, 2, 3, and 4 incidents will be detailed in the report, accompanied by a current status of the incident.

Detailed Follow-up Reports: These reports are initiated by the severity rating assignments, and will be required by the [Computer Incident Response Team / IRT / Steering Committee] until any incident above Level 0 is closed as fully investigated. They must include all information described in the response process above.
Other reports to consider:

- Incidents Per Month
- Total Alerts
- Ticket Summary
- Pie Chart showing Severity Ratings

[Computer Incident Response Team / IRT / Steering Committee] Meeting Agenda and Minutes

The Information Security Officer will create a [Computer Incident Response Team / IRT / Steering Committee] Meeting Agenda and distribute that to all [Computer Incident Response Team / IRT / Steering Committee] members in advance of the quarterly meeting. The Information Security Officer will distribute minutes of the [Computer Incident Response Team / IRT / Steering Committee] meeting within one week of the meeting. Minutes will be distributed to all [Computer Incident Response Team / IRT / Steering Committee] members[. / as well as [the Board of Directors / the Audit Committee / the CIO / the President / list others here].

Retention of Reports and Supporting Documentation

All [Computer Incident Response Team / IRT / Steering Committee] reports, Suspicious Activity Reports, and IDS alerts not deemed as false positives must be kept permanently by the Information Security Officer.

Shared Passwords:

Passwords that, unlike user-level Network or Application passwords, that should be known by more than one individual, also should be documented. Examples of these passwords include Web Domain Name Registrars, Web Hosting administrator passwords, router passwords, administrator passwords on workstations, etc.

Some of these passwords may be shared with the MSSP and and/or third-party Network Support Providers. For example, firewall management may be outsourced, and thus the credentials necessary to manage the firewall should be shared and documented. Also, given that the persons responsible for

clearing IDS alerts are usually authorized to respond to true incidents in real time, most password management procedures include methods to make these passwords available to those in the Network Operations Center (NOC) that watches and clears IDS alerts.

Name of Financial Institution documents shared passwords as per the Password Management Procedure.

Information Disclosure

Information gathered by the Intrusion Detection System and other Security Devices may only be disclosed to the Information Security Officer, the [Computer Incident Response Team / IRT / Steering Committee], and Management. Disclosing information to any other party (including other employees, regulatory agencies, law enforcement, third-party vendors other than the MSSP who gathers the information, and the media) may be done only with the approval of Management. The MSSP is required to have a nondisclosure agreement on file.

Disclosure as required by law to regulatory bodies will be handled by the Information Security Officer or the Internal Auditor / Compliance Officer and does NOT need the express approval of management.

Incident Tracking

The Information Security Officer will document incidents during the Triage process, and any incidents classified as Security or Disclosure will be documented until they are closed. An incident log is used. Metrics to track during an incident include:

- Time and Date of Incident
- Broadcast Awareness Time
- Time / Date of Containment
- # of Records
- Scope of breach (list of data fields)

Incident Response Team Training Tools

The following “tools” are available for training the Incident Response Team:

- The Incident Response Policy
- This Plan, for which we perform an annual walk-through’s
- Incident Response Tests, required by policy
- Decision Trees, Scenario Descriptions, Virus Removal Procedure, Compromised Credential Procedures
- NIST SP 800-61, The NIST CyberSecurity Framework
- FIL 2005-27, the FFIEC Statement on Compromised Credentials, the FFIEC Statement on Destructive Malware, and our State CATO Guidance.
- Generic Talking Points
- Generic Media Strategy
- “Incident Response Simplified” . . . a PowerPoint by Infotex.

Distribution of Potential Incident Reporting Guidelines to Technology Team

The information in Appendix A relates to the reporting of Suspicious Activities or Potential Incident Reports (PIRs) by regular members of the Information Technology Team. The Information Security Officer may distribute Appendix B to team members or, if appropriate, distribute the entire Incident Response Plan. However, annually, all technology team members must be reminded of the procedures defined in the Appendix, and the actual Potential Incident Report form must be distributed.

Concluding Sections

The following sections may or may not apply to your institution, depending upon your own policy/procedure development protocols. However, we do strongly urge you to include the distribution list, policy owner, and policy reviewers sections for your convenience and to ensure appropriate review and training. Please remove this section.

Reporting to the Board of Directors

The [Information Security Officer / Internal Auditor] will report to the Board of Directors on an annual basis that all procedures listed above have been reviewed for completion, enforcement, and training. Specifically, this report will indicate that all procedures listed above have been updated. The report will list deficiencies related to enforcement of the policies and procedures above, as well as indicate the level of training provided to members of the various teams affected by the policies and procedures listed above. The Board of Directors will also receive summary reports of examinations, audits, and other assessments of the risk inherent in information security as they are required.

Noncompliance

Violation of these procedures may result in disciplinary action which may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Name of Financial Institution's information resources access privileges, and civil and/or criminal prosecution.

Storage of Policies, Procedures and Standards

The Information Security Officer is responsible for maintaining current copies of all information security related policies and procedures. These will be stored [state method and location] and an electronic copy will be stored off-site [state location]. The electronic copy will be updated annually (in December) as well as on an as-needed basis any time there is a major revision of a particular policy or procedure.

Plan Training

The Information Security Officer, Network Administrator, and Senior Management will review this plan annually and hold training to ensure that all appropriate personnel understands the provisions of this procedure, as well as the implications upon their job description responsibilities.

Contribution to Control Objectives for Information Technology

Enforcement of this procedure contributes to the achievement of CobiT:

- PO9: Assess and manage IT risks.
- DS8: Manage service desk and incidents.
- DS10: Manage problems.
- ME2: Monitor and evaluate internal control.

Distribution List

The following positions will receive this procedure and any changes to this procedure:

- All Members of the [Computer Incident Response Team / IRT / Steering Committee]
- All [Information Technology Team Members] will receive the Guidelines for Reporting Suspicious Activities section.
- List those individuals. Consider establishing an e-mail alias corresponding to the individuals.

Plan Owner

- Title Here

Plan Reviewers

- Titles Here

Related Policies / Procedures / Tools

- [Computer Incident Response Team / IRT / Steering Committee] Meeting Procedure
- [Computer Incident Response Team / IRT / Steering Committee] Training Presentation
- Incident Response Decision Tree
- Incident Response Plan
- Incident Response Policy
- Intrusion Detection Procedure
- Password Management Procedure
- Potential Incident Report
- Suspicious Activity Report (SAR)
- Third Party Information Request Procedure
- Virus Incident Response Procedure
- Web Defacement Procedure

Appendix A: Guidelines to Report Observed Suspicious Activity

Members of the [Information Technology Team] are in a unique position to notice "suspicious activity" such as offensive materials stored on workstations, policy violations, and/or hacker activity. These observations must go into the reporting pool overseen by the [Computer Incident Response Team / IRT / Steering Committee]. Suspicious activity should be reported internally using a Potential Incident Report (PIR) (Appendix D). Notifications could come directly to the [Computer Incident Response Team, ISO] from a source other than an Information Technology Team Member (e.g. MSSP, vendor, contract employee, associate from another department). In such an event, the [Computer Incident Response Team, ISO] should initiate Potential Incident Report (PIR) as described in this document.

Responsibilities

1. Each member of the [Information Technology Team] is responsible for identifying potential suspicious activity and to follow the following guidelines for reporting suspicious activity.

2. Members of the [Information Technology Team] are responsible for reporting any suspicious activity to the [ISO] as defined in this procedure. In the case of urgent incidents, if the [ISO] is unavailable the team member should notify any member of the [Computer Incident Response Team / IRT / Steering Committee] using the PIR defined in this procedure.

3. Upon receiving a PIR, the ISO is responsible for determining the severity level of the incident and conducting escalated research for each instance of suspicious activity following the procedures defined in this plan (containment, eradication, recovery, and follow-up.)

4. The ISO will document the results of the research and submit the information to the [Computer Incident Response Team / IRT / Steering Committee] within [5] business days of initial detection of the suspicious activity.

5. The ISO will maintain a file of all PIRs including both forms submitted to the [Computer Incident Response Team / IRT / Steering Committee] for further action as well as forms that were determined to be "false positives" or low-level Severity Ratings. These records (along with all [Computer Incident Response Team / IRT / Steering Committee] reports) must be kept permanently.

6. The ISO is responsible for distributing and training Information Technology Team members on the Suspicious Activity Report on an annual basis.

Confidentiality

Disclosure of information concerning an investigation to any person involved in the suspected activity or any other person that does not require that information to fulfill the duties of their job may be grounds for disciplinary action up to and including termination. Likewise, the [Computer Incident Response Team / IRT / Steering Committee] will not disclose the source of a PIR outside of the [Computer Incident Response Team / IRT / Steering Committee] and bank management without a specific legal purpose or a specific documented business reason, and such disclosure will not happen until after the team member initiating the report is informed.

Suspicious Activity Triggers

The following is only meant for example purpose and not intended to be all-inclusive. Team members are encouraged to report any activity they feel is suspicious, and are not discouraged from reporting activities that are later deemed "false positives."

1. While performing maintenance on a workstation, you observe files stored on the workstation that would be considered offensive or illegal.
2. You notice that an employee has written a password down and is storing the password in an easily accessible place, such as under the keyboard or on the monitor.
3. You notice spyware on a workstation.
4. An individual attempts to gain access to the network, applications, or electronic data without going through the normal access management process.
5. You are the recipient of forwarded jokes, e-chain letters, etc.
6. An individual asks to have their password reset or changed and they can not provide the required identifying information.
7. You observe an individual copying data to an external storage device such as a floppy disk, CDROM, or USB Drive that does not seem consistent with their job role or that is prohibited as per the Acceptable Use Policy.
8. The virus management software reports a virus attack.
9. Network monitoring tools or logs show unusual activity. Network logs show attempts to login with repeated occurrences of invalid passwords, or attempts to access administrator accounts.
10. You observe an individual accessing an application system in a manner you do not feel is consistent with the scope of their job. For example, you observe an individual in a loan area accessing deposit information.
11. You observe or become aware of someone using non-Bank owned or unauthorized software on a workstation or server.
12. You observe an individual using a laptop connected to the Bank network that you know is not a bank device.
13. You observe individual downloading/exporting information from Bank Systems that you do not feel is consistent with their job role.
14. A branch manager informs you that a "telephone repairman" attempted to access the network closet and, when told to wait for confirmation, left the branch.

Examples of Reportable Incidents

The following are examples of reportable incidents.

1. Using another person's individual password and/or account information.
2. Failure to protect passwords and/or access codes (e.g. sharing individual codes; taping to equipment to avoid memorizing).
3. Accessing customer records for other than a "need to know" reason.
4. Asking unauthorized personnel to access your personal record/data.
5. Unauthorized personnel accessing a co-workers record in response to their request.
6. Leaving a workstation signed on/unattended; failure to log off.
7. Unscheduled system downtime.
8. Unauthorized use of external computer connections (e.g. modems).
9. Installation of unauthorized software (screensavers, games, etc.).
10. Indication of computer virus.
11. Illegal reproduction of customer data.
12. Inappropriate disposal of customer data.
13. Falsifying data (customer, financial, employee, mission critical, etc.).
14. Disclosing customer information with unauthorized personnel; failure to safeguard confidential data.
15. Theft of computer equipment or software.
16. Inappropriate use of software, such as illegal copying of licensed computer software, intentional introduction of computer viruses, etc.
17. Inappropriate use of the Internet.
18. Inappropriate use of e-mail.
19. Defacing the financial institution's website.
20. Destruction or tampering with the financial institution's equipment.
21. Negative post by a customer or non-employee on a Social Media Site.
22. Negative post by an employee on a Social Media Site.

Appendix B: Response Scenarios

Note: Appendix B is meant for larger banks and is based on the FFIEC guidelines for Disaster Recovery Testing, though no such guidelines currently existing for "security incidents."

The following are incident scenarios with a high likelihood as per our risk assessment process, and therefore we have developed response plans specific to the incident:

1. Phishing Attack
2. Accidental Leak of Data
3. Corporate Account Takeover
4. DDoS Attack
5. Vendor Incidents

1. Phishing Attack

2. Accidental Leak of Data

3. Corporate Account Takeover

Incident Response Plan for Account Takeovers

- Make sure appropriate employees are trained on account takeovers, with the following considerations:
  - Those in the ACH, Wire Transfer, and Billpay detect and response function should be included in this training.
  - A high level version of the training should be provided to management and the board.
  - Training should address:
    - What is a Corporate Account Takeover
    - What are the most common attack vectors
      - Malware (viruses, worms, keyloggers, remote control)
        - Drive-by sites, E-mail, Mobile Apps
      - Rogue Software, Fake AntiVirus, Scareware
      - Phishing, Spear Phishing, Phone Phishing, Vishing, Smishing
      - Orchestrated Attacks, Zeus, Zitmo
    - Anatomy of an Attack
      - Malware
      - Targeting
      - Monitoring
      - Execution (transfer of funds0
    - Incident Response Plan

- Detection
  - Relationship to DDoS
- Containment
- Response
- Notification

4. DDoS Attack

DDoS attacks are frequently targeted towards financial institutions. DDoS can affect the institution in a number of ways. <Name of Financial Institution> has evaluated the various scenarios that can occur regarding DDoS. The following is our plan for responding to a DDoS attack.

Definition of Denial of Service

A **denial-of-service attack** (**DoS**) or **distributed denial-of-service attack** (**DDoS**) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or group of persons to prevent an internet site or service from functioning efficiently or at all, temporarily or indefinitely. A distributed denial of service attack leverages groups of attack devices so that the effect of the attack is greater, and so that containing the attack is more difficult. Perpetrators of DDoS attacks typically target sites or services hosted on high-profile web servers . . . such as banks. In recent years, DDoS attacks on banks have increased in number and visibility, to the point where regulators are starting to supervise banks' response efforts. In <Name of Financial Institution>'s environment, most of the typically attacked assets (applications, products, and services) are hosted by third parties, and thus will require their involvement in resolution.

Definition of Detect and Response Personnel

<Name of Financial Institution> has identified certain personnel to fulfill the role of "detect and response," meaning they monitor (looking for anomalies and responding to monitoring systems), investigate (looking for fraudulent transactions), and approve transactions in the areas of billpay, ach origination, and wire transfer (list any other assets if appropriate). For the purposes of this plan, the following positions are considered to be "detect and response personnel"

- Position Name E-mail Address Phone Number Assets (define which transactions they protect)
- Position Name E-mail Address Phone Number Assets (define which transactions they protect)
- Position Name E-mail Address Phone Number Assets (define which transactions they protect)
- Position Name E-mail Address Phone Number Assets (define which transactions they protect)

Proactive Controls

To refresh the Incident Response Team's memory during the panic of an actual DDoS incident, the following controls are in place to prevent, detect, or mitigate a DDoS attack:

(List any controls you may have. If you have none, delete this section. Examples are as follows.)

- **AT&T Internet Protect Service with DDoS Defense** (or anything that may be provided by your ISP)
- **Critical Clients are whitelisted.**
- **We have established a "hidden door," that can be opened during a DDoS attack to allow access to those whom we deem necessary during the attack. It is important to know that this door could be discovered by the attackers and become unavailable during the attack.**
- **We have established a "back door exit" which can be opened during a DDoS attack to allow our employees internet access during the attack. It is important to know that this door could be discovered by the attackers and become unavailable during the attack.**
- **We have retained <name of firm> for IP scrubbing.**

Response Process:

For all DDoS or DoS attacks, a predictable life cycle should be as follows:

1) Initiation: The attack is initiated. Normal systems, services, and functionality slow.
2) Detection: <Name of Financial Institution> detects the attack.
3) Mitigation: A response is implemented which may include blocking, contingency implementation, and/or communication.
4) Containment: The Information Security Officer declares that the attack has been contained.
5) Analysis: A "post mortem" analysis is conducted and this plan is updated.
6) Monitoring: The Information Security Officer will continue monitoring for signs of re-initiation.

Meanwhile, there are two primary response processes: one for in-house assets, and one for outsourced assets.

Response Process: In-House Assets

Detection:

The reactive way to detect a DDoS or DoS attack against the bank's network is to experience a slowdown or complete stoppage of services trying to access the internet or trying to access the internal network through the internet. To proactively detect a DDoS attack, <Name of Financial Institution>'s Managed Security Service Provider (MSSP) will provide assistance in identifying and remediating attacks. . The IT Helpdesk will serve as a central point of contact for reporting any suspected DDoS type attacks. The Information Security Officer will officially declare whether <Name of Financial Institution> is undergoing an attack and, upon such declaration, mitigation will begin.

Mitigation

1. Initial Investigation
   a. Shut down affected services to determine the scope of the attack and, if possible the source(s).
   b. Work with the MSSP and firewall administrators to determine where the traffic is coming from.
   c. The above two steps could take place prior to declaration of an attack by the Information Security Officer.
2. React, Defend, and Contain!!
   d. If it is determined that any services are non-essential they may remain shut down until containment.
   e. Obtain assistance from the MSSP in blocking the attack if possible.
   f. Recognize that some customers may be legitimately overseas. Blocking all traffic from outside the US might be a good start, but it will have some problems.
   g. Re-direct DNS records to different addresses in order to bring services back up.
   h. If IP scrubbing services have been retained, document process to initiate scrubbing here.
3. Contingency Implementation
   a. Given the potential for disruption of services that can occur during a DDoS attack, Business Continuity Plan (BCP) processes may be utilized to continue service to customers.
   b. If backdoor exits have been established, initiating the rerouting would be documented here.
   c. Walk through each asset identified in the asset inventory below, and address how we can overcome a DDoS attack in this section. See e-mail below as an example.
   d. E-mail: Document a method, if any, to reroute e-mail during an attack. For example: **SMTP mail service is directed to** <document here.> **In a DDoS scenario, the MX record can be re-directed to an alternate method in order to continue to receive email services.** <Name of Financial Institution>**'s Firewall is configured to only accept smtp traffic from the** <name of spam filtering service> **filtering service to reduce the possibility of email floods.**
4. Communicate, if necessary:
   a. The Information Security Officer will inform the Incident Response Team
   b. The Information Security Officer will notify detect and response personnel.
   c. The Information Security Officer will work with the I.T. Infrastructure & Information Security units to communicate expectations of technology users; which systems can safely be used, the workaround procedures which should be implemented, and what additional precautions may need to be put in place. Information will be disseminated as quickly as appropriate based on input from the other technology units and the Incident Response Team, and ONLY after is has been confirmed as factual and not speculation.
   d. Detect and Response Personnel will heighten awareness in ACH, Wire Transfer, and Billpay

fraud detection processing.

e. In the event that services become unavailable to customers due to a DDoS attack, <Name of Financial Institution> will communicate with customers via available channels such as phone, email, Social Media, News Media, in person at financial center locations, etc. See communication standards below.

Containment:

The Information Security Officer is authorized to declare when an attack has been properly contained. This is no light matter. How long to stay in mitigation depends upon the situation. Sometimes waiting only 24-48 hours after the attack is over is sufficient. Other times companies stay in mitigation for weeks. The implications of this declaration is that data owners and detect and response personnel do not have to continue with the heightened awareness. Blocks are allowed to expire and traffic returns to normal routing. It takes time after mitigation to return to normal.

This declaration will be accompanied with a proposed date for the Post-Mortem Analysis meeting.

Any follow-up communication with customers, law enforcement, the media, etc. will be handled with the guidance of the Incident Response Team.

It is important to know proactively that most organizations who have suffered a DDoS attack report that it takes time to "come back to normal."

Analysis:

Post-Mortem analysis should try to document how well the response went, what could be done better, what should be done again, who might have implemented the attacks, and what issues are still open resulting from the attack (such as a corporate account takeover). If necessary, this plan will be updated.

The effectiveness of reaction tools (such as back door exits and/or IP Scrubbing services) should also be included in the analysis, and plans to adjust such tools should be finalized. (For example, if a back door exit was used to circumvent an attack, do the attackers now know of such a back door, and thus should a new back door be constructed?)

Forensic evidence should be reviewed and the results of the review presented to the Incident Response Team, who will determine if further investigation is warranted. Evidence will be properly stored (to the degree that is possible) by the Information Security Officer.

Monitoring:

The fact that there was one DDoS attack often means there might be another. The Information Security Officer will work with the Managed Security Service Provider and other organizations to monitor for an additional attack. Furthermore, any action items arising from the analysis process will be tracked by the Information Security Officer until brought to adequate resolution.

Response Process: Outsourced Assets

Detection:

The reactive way to detect a DDoS or DoS attack against the bank's network is to experience a slowdown or complete stoppage of services that unfortunately are mostly customer-facing services. In other words, detection may come in the form of customer complaints. There really is no way to proactively detect a DDoS attack on outsourced assets. We would hope that our vendors will contact us in the event they are experiencing a DDoS attack. However, we should not expect it, as a vendor may decide to delay communication longer than we would want. The IT Helpdesk will serve as a central point of contact for reporting any suspected DDoS type attacks. The Information Security Officer will officially declare whether <Name of Financial Institution> is undergoing an attack via an outsourced asset as well as which asset is undergoing the attack and, upon such declaration, mitigation will begin.

Mitigation

1. Initial Investigation: [Data / System / Application] and Vendor Owners will probably be the first management team member to become aware of the issue, and must be trained to immediately inform the Information Security Officer. They will then need to work with the appropriate staff to establish lines of communication.
2. Response: The direct response to the attack will be performed by the vendor.
3. Contingency Implementation
    a. Given the potential for disruption of services that can occur during a DDoS attack, Business Continuity Plan (BCP) processes may be utilized to continue service to customers.
    b. System restoration priorities will be approved by the Incident Response Team, but will also be based in part on the Business Impact Analysis and other prioritization processes inherent in the Business Continuity Plan.
    c. Vendor Owners should ask vendors about potential contingencies during vendor due diligence. The Information Security Officer will quiz the vendor about contingencies during the attack.
    d. Walk through each asset identified in the asset inventory below, and address how we can overcome a DDoS attack in this section. See e-mail below as an example.
    e. <Name of Financial Institution>'s customer facing Marketing website is hosted by a 3rd party provider that monitors web traffic to identify DDoS attack patterns. The website host has a notification process in place when there are disruptions in service as well as DDoS specific mitigation procedures.
    f. <Name of Financial Institution>'s Online Banking application is hosted by Fiserv. Fiserv has procedures in place for identifying and mitigating DDoS specific attacks. This process has been shared with client institutions and has been determined that it is a reasonable strategy.
4. Communicate, if necessary:
    a. The Information Security Officer will inform the Incident Response Team
    b. The Information Security Officer will notify detect and response personnel. Note: Even if the attack is on non-bank owned assets, we believe that detect and response personnel should be notified.
    c. The Information Security Officer will work with the I.T. Infrastructure & Information Security units to communicate expectations of technology users; which systems can safely be used, the workaround procedures which should be implemented, and what additional precautions may

need to be put in place. Information will be disseminated as quickly as appropriate based on input from the other technology units and the Incident Response Team, and ONLY after is has been confirmed as factual and not speculation.

d. Detect and Response Personnel will heighten awareness in ACH, Wire Transfer, and Billpay fraud detection processing.
e. In the event that services become unavailable to customers due to a DDoS attack, <Name of Financial Institution> will communicate with customers via available channels such as phone, email, Social Media, News Media, in person at financial center locations, etc. See communication standards below.

Containment:

The Information Security Officer is authorized to declare when an attack has been properly contained. The implications of this declaration is that data owners and detect and response personnel do not have to continue with the heightened awareness. This declaration will be accompanied with a proposed date for the Post-Mortem Analysis meeting.

Any follow-up communication with customers, law enforcement, the media, etc. will be handled with the guidance of the Incident Response Team.

Analysis:

Post-Mortem analysis should try to document how well the response went, what could be done better, what should be done again, who might have implemented the attacks, and what issues are still open resulting from the attack (such as a corporate account takeover). If necessary, this plan will be updated.

The effectiveness of the vendor's role in the response should be evaluated as well as communication channels, recovery time objectives, and customer concerns.

Monitoring:

The fact that there was one DDoS attack often means there might be another. The Information Security Officer will work with the affected vendor to monitor for an additional attack. Furthermore, any action items arising from the analysis process will be tracked by the Information Security Officer until brought to adequate resolution.

Communication Standards

Guiding principles for communication during an attack include:

- DDoS is not "being hacked." There are no regulations governing notification requirements for DDoS. We are not required by law to inform customers that we are under a DDoS attack.
- Be sure to avoid communicating speculation. Only communicate facts.
- Acknowledge a degradation of service.
- Be sure to point out that there has not been a breach of security.
- It's important to know that any kind of attack and mitigation will change the customer experience. Customers will be frustrated and at the end of their patience.

The Information Security Officer will work with [the IT Department / the Technical Team / Network Support] to communicate expectations of technology users; which systems can safely be used, the workaround procedures which should be implemented, and what additional precautions may need to be put in place. Information will be disseminated as quickly as appropriate based on input from the other technology units and the Incident Response Team, and ONLY after is has been confirmed as factual and not speculation.

Communication must be very careful in that if we tell our customers we are under a DDoS attack, they may think this means we are being hacked, and that their funds are at risk. Better terminology may include "systems are experiencing degradation due to circumstances beyond our control."

The Incident Response Team will clear content of communication and, through the coordination of the Information Security Officer and the Marketing Director, will make available "incident talking points" to key team members during an incident. A template for these talking points is on file. At this time, we don't believe a press release would be warranted by a DDoS attack, and thus there is no template available for this.

Contact Information for a DDoS attack:

- (xxx) yyy-zzzz Help Desk
- (xxx) yyy-zzzz Information Security Officer
- (xxx) yyy-zzzz <Chief Information Officer / VP of IT / Director of IT>
- (xxx) yyy-zzzz Internet Service Provider
- (xxx) yyy-zzzz Managed Security Service Provider
- (xxx) yyy-zzzz IP Scrubbing Provider
- (xxx) yyy-zzzz Billpay Fraud Detection Personnel
- (xxx) yyy-zzzz Wire Transfer Fraud Detection Personnel
- (xxx) yyy-zzzz ACH Fraud Detection Personnel

Vendor Owners will be responsible for providing contact information so that the Incident Response Team can correspond effectively with appropriate vendor personnel during an attack on outsourced assets.

Inventory of Exposed Assets

Assets exposed to DDoS Attack (from a high likelihood perspective) include two primary categories from a response perspective: those assets which are accessed through the perimeter of the bank's network (in-house) and those assets which are hosted at a third party data center (outsourced.)::

In-House:

The following assets are accessed through the perimeter of the bank network, and would be exposed to a DDoS attack on the bank:

- E-mail
- Intranet
- General Internet Access
- Telephone Systems
- ACH Transaction Processing
- Wire Transfer Processing
- Microsoft Outlook Web Access (OWA)
- Connection to Core
- VPN Access
- Portals and Websites (consider breaking this down, ie: 401k Websites, Payroll Portal, Fedline, etc.)

Outsourced Assets:

The following are assets that would be exposed to a DDoS attack on a third party:

- Commercial Internet Banking
  - Commercial ACH Origination
  - Commercial Wire Transfer Origination
  - Commercial Billpay
  - Commercial Electronic Funds Transfer
  - E-Pay: Add a Vendor
  - Change Password on Account
  - Change Username on Account
  - Remember Password
  - E-Pay: Pay a bill
  - Change E-mail Address on Account
  - Chat with Helpdesk (Customer Service)
  - Transfer Funds Within Customer Accounts
  - Login to Account
  - Change Address Initiated by Customer but handled by Bank Employee
  - Change Phone Number on Account
  - Check Balance
  - Stop Payment
  - Remove Authorized Access to an Account
  - View Account History
  - View Account Summary
  - Electronic Banking Maintenance Forms (customer setup changes, customer password changes)

- Remote Capture Deposit
- Mobile Banking
  - Billpay
  - Consumer Capture
  - Consumer Electronic Funds Transfer
  - Downloading Mobile Banking App from the Application Market
  - New User Registration
  - P2P Payments, Zashcash, etc.
- Retail Internet Banking
  - Consumer ACH Transactions
  - Change Password on Account
  - Forgot My Password
  - Change Username on Account
  - E-Pay: Add a Vendor
  - Add People to Account
  - Internet Banking Consumer Customer Interface
  - Change Password Initiated by Customer
  - Login to Account
  - Change E-mail Address on Account
  - E-Pay: Pay a bill
  - Chat with Helpdesk (Customer Service)
  - Internet Banking Secure Chat Feature
  - Change Address Initiated by Customer
  - Change Address on Account
  - Change Phone Number on Account
  - Transfer Funds Within Customer Accounts
  - Apply for Loan
  - View Account History
  - E-statements
  - View Account Summary
  - Bill-pay Administrator Accounts
  - On-line Banking Administrator Access
  - Sign up for E-statements
  - Request Alerts
  - Stop Payment
  - Electronic Banking Maintenance Forms (customer setup changes, customer password changes)
  - Secure Chat Application
- Other Third Party Hosting Providers
  - Hosted E-mail Providers
  - Hot Site or other Disaster Recovery Sites
  - Managed Service Providers (such as IPS/IDS providers)
  - Google (ie: if using Google Docs or Google Apps for e-mail and calendaring)
  - Marketing Site (an attack on the web hosting company)

Responsibilities of the Information Security Officer during a DDoS Attack

1. The Information Security Officer declares that an attack is underway, coordinates the Incident Response Team during the mitigation and contingency implementation process, declares when containment has been achieved, and orchestrates the analysis and monitoring processes.

2. When notified, the Information Security Officer performs a preliminary analysis of the facts and assesses the situation to determine the nature and scope of the incident.

3. The Information Security Officer must put all appropriate employees on notice, especially those who are provide fraud detection functionality for the institution. DDoS attacks have shown to be a diversionary tactic in order to draw attention away to initiate intrusion, data breach, and financial fraud activities.

4. The Information Security Officer will then review the preliminary details with other appropriate technical personnel to determine a course of action – including additional diagnosis to determine the scope of the DDoS event, whether it is continuing or not and research for patches, fixes and remediation.

5. If there is the potential for a privacy breach or other intrusion, refer to those sections of this document.

6. The Information Security Officer is responsible for documenting all details of an incident and facilitating communication to executive management and other auxiliary members as needed.

7. The Information Security Officer will contact all appropriate <data / system / database / system> owners and system administrators to inform them of the attack and the mitigation effort, and to determine the scope of the DDoS event. One objective of this is to share information relating to what to watch out for, what tasks can still safely be conducted, and how to assure non-compromised systems can stay that way.

8. Forensics evidence is difficult to manage in a DDoS attack but during an in-house attack the Information Security Officer will consider preservation of evidence to be used in the post-mortem analysis.

9. Then the Information Security Officer will contact appropriate Incident Response Team members (First-Level Escalation members).

10. The Information Security Officer will direct and coordinate all activities involved with Incident Response Team members in determining the details of the DDoS event.

11. Throughout the attack, the Information Security Officer will be working with appropriate external parties (law enforcement, the MSSP, IP Scrubbers, other technical vendors) to take measures to stop or control the DDoS attack; and collect and preserve appropriate information to aid investigative efforts.

12. If an internal user (authorized or unauthorized employee, contractor, consultant, etc.) appears connected with the DDoS event, the Information Security Officer will contact the Human Resources Manager for possible disciplinary action or termination. In the case of contractors, temporaries, or other third-party personnel, the Information Security Officer will ensure discontinuance of the vendor's access and contact the appropriate vendor owner.

Responsibilities of Data / System / Application and Vendor Owners During a DDoS Attack:

1. All <Data / System / Application> and Vendor Owners will be trained on what a DDoS attack is and what their responsibilities will be during a DDoS Response Scenario.

2. If <Data / System / Application> and Vendor Owners identify a potential DDoS disruption to access to their systems, the <Information Security Officer / CIO / IT Helpdesk> should be contacted immediately with all available information to ensure that the appropriate Incident Response Team members are notified.

3. For outsourced systems, the <Data / System / Application> and/or Vendor Owner of the affected system will coordinate and establish a communication connection between the Information Security Officer and the appropriate vendor contact who will answer questions and help with communication.

4. <Data / System / Application> and Vendor Owners should quickly evaluate the implications of the DDoS attack, particularly if data loss is involved, and implement alternate work procedures where necessary to minimize the potential for continued disruption or fraudulent access. <Data / System / Application> owners should keep <the Information Security Officer / technical support / the CIO> informed as appropriate.

5. <Data / System / Application> and Vendor Owners should work with the Information Security Officer and the Incident Response Team to contact any third parties that could be impacted or could provide reasonable levels of assistance (if warranted).

6. <Data / System / Application> and Vendor Owners should assist in determining priorities for granting access to third parties such as customers. The Incident Response Team determines priorities for system restoration.

Incident Response Team Responsibilities

1. After confirmation that an incident has occurred or is occurring, the Incident Response Team should notify appropriate executives which may include the CEO, legal counsel, board members, etc.

2. The Incident Response Team should provide guidance in communicating with third parties, including the media, customers, law enforcement, and vendors. The Incident Response Team should approve content of communication whenever possible.

3. The Incident Response Team will determine restoration priorities using the Business Impact Analysis as a guideline.

4. If necessary, the Incident Response Team will decide when it is necessary to notify the appropriate authorities (e.g., Local Law Enforcement, FBI, Federal Trade Commission (FTC), etc.)

5. The Incident Response Team will determine when it is appropriate to notify customers and will provide guidance on the content of such notification.

6. The Incident Response Team will determine if any legal action is possible and pursue accordingly.

Responsibilities of the <Technology Team / IT Department / Infrastructure Team>

1. Responding to a DDoS incident will take high priority over all projects and regular duties unless other actions are approved by the <CIO / Information Security Officer / IT Manager / COO / VP of IT>.

2. As quickly as possible, the <IT Department / Technology Team> will implement appropriate patches and security changes to remediate any continuing vulnerabilities that may have been exploited with DDoS attack.

3. When notified that a DDoS attack may be underway, <IT, the Technology Team> will immediately implement procedures to minimize further risk from the intrusion. These measures could include rerouting of traffic, reconfiguring of mx records, initiation of IP scrubbing, etc. Measures will be approved by the <CIO / Information Security Officer / IT Manager / COO / VP of IT>.before implementation. The <IT Department / the Technology Team> will work with the Information Security Officer and Incident Response Team on potential added security measures.

4. The <IT Department / Technology Team> will contact technology providers for assistance as appropriate and as requested by the Information Security Officer or members of the Incident Response Team.

5. The <IT Department / Technology Team> will implement appropriate authorization access resets for any compromised system IDs.

6. The <IT Department / Technology Team> will participate in the analysis and monitoring processes defined above.

Marketing / Public Relations Responsibilities

1. When requested, the Marketing Coordinator will prepare appropriate response to media, customer, and/or employees. The Incident Response Team must approve prior to distribution (pursuant to crisis plan).

2. The Marketing Coordinator will coordinate responses to media inquiries, if necessary; and monitor media coverage and circulate accordingly; assure that only appropriately approved communications are being disseminated.

Responsibilities of the Managed Security Services Provider (MSSP)

Note: We encourage you to run this by your MSSP to ensure that it is accurate.

1. The MSSP can only directly help with devices and systems hosted “in house” by the bank, and not those outsourced to other providers.

2. Most DDoS attacks can be potentially blocked or at least detected by the Intrusion Prevention Systems (IPS) and the Intrusion Detection Systems (IDS) maintained by the MSSP and monitored 24x7x365.

3. IPS/IDS systems act as an additional layer of perimeter defense. Port scans are blocked by IPS maintained by the MSSP. Unpredictable attack vectors should be detected by the MSSP.

4. Because of the volume of port scans occurring in any given day, the MSSP does not report every time an IP address is blocked, so contact should be made to assess and assure blocking is begun. However, when the automated IPS software detects an IP address is scanning for open firewall ports, the MSSP software automatically blocks that IP address for a period of time.

5. Any unusual scanning activity occurring inside the network will be detected (and reported in real time) by the MSSP according to a Calling Tree that is maintained by the team.

6. During the containment phase of a network intrusion event, the MSSP will work with the team to provide information that may be available in the network traffic history as well as in the event logs.

7. If the MSSP was NOT able to block malicious traffic, or report on malicious traffic occurring in the internal network, an investigation must be launched to determine if a failure occurred on the IPS/IDS/ELM controls that are in place. The MSSP will work with the team to ensure that information is appropriately and quickly provided to document viability and effectiveness of controls.

5. Vendor Incidents

Incidents created by vendors are unfortunately highly likely and often come with a high impact. The Vendor Management Policy requires certain disclosure agreements so that in the event there is a negative incident caused by or perpetrated at a vendor, the bank should receive timely notice.

When the institution receives notice from a vendor that a breach has occurred, procedures already established in this document must be followed. Immediately upon receipt of the notice, the Information Security Officer will assess the extent of the damage (impact) considering factors such as the number of customers affected, the type of information breached, the transactional capability of the breach, etc.) Once a complete understanding of the impact is reached, the Information Security Officer will then act according to this procedure.

Appendix C: Guidelines for Monitoring Employee Behavior in the Public Presence

As employers, financial institutions have valid reasons to establish policies relating to employees' use of social media websites such as Facebook and Twitter. First, there is an interest in preventing its employees from focusing their attention (to some, an all-consuming attention) on their social blogs. Not only may such activity detract from productivity, it may introduce inappropriate content into the workplace.

Second, a financial institution has an interest in monitoring what is said about its business. Disgruntled employees may publish unfavorable opinions about the employer (or even its customers) via social websites. For these reasons, an employer can and should provide guidelines to its employees who utilize social media.

It is important that we recognize the monitoring of social media is different than the monitoring of Name of Financial Institution-owned networks in that we are watching what our employees do "in public," after they have "left the office."

Still, reputational risk from policy violations by employees or misrepresentation and other defamatory statements by former employees is a reality, whether we want it to be or not.

Though monitoring what employees do off company property presents some legal risk (violation of privacy laws), there is no law against monitoring what is being said about Name of Financial Institution. Thus, the following is a method of monitoring activity in a manner that does not invade privacy.

Therefore, Name of Financial Institution will identify a Monitor who would be responsible for performing searches on a regular basis. The results of these searches should be reviewed and reported to the [Computer Incident Response Team / IRT / Steering Committee] on a regular basis.

The Information Security Officer should run extensive searches on both major search engines (such as Google, Bing, and Yahoo) and in each of the major social media sites (listed below). The searches should look for Name of Financial Institution's name and variations of the financial institution's name. The searches should be run prior to each [Computer Incident Response Team / IRT / Steering Committee] , IS Steering, Executive Committee meeting and bring any concerning results into the meeting. Examples of "concerning results" include:

- Policy breaches by current employees.
- Negative posts by previous employees, customers, or other persons.
- Similar uses of the financial institution's name by other corporations
- Anything that would affect Name of Financial Institution's reputation or security in a negative manner

For the purpose of monitoring, the following are considered to be "major social media sites:"

- Facebook
- LinkedIn
- Myspace
- YouTube
- Flickr
- Twitter

Monitoring Tools: (note, this is as of 2009)
Monitter.com allows you to customize Twitter searches by keyword and location and save your searches as RSS feeds to have the data emailed or texted to you instantly. Start off slow with searches for the bank name or a new product and monitor twitter for threats, disgruntle employees and internal leaks. Do NOT monitor for individual employee names unless management has approved.

Addictomatic.com provides a quick and easy way to search for your company or keywords across a wide selection of sites including news, blogs, YouTube, and even popular photo-sharing site flickr. Countless unapproved videos and photos by employees can quickly be discovered.
All employees should be encouraged to use metadata in sensitive documents or documents that could be considered intellectual property. The term "Confidential Handling" should be placed in the metadata.

Google's proprietary collection of websites and vast arsenal of tools can be used for monitoring social media usage. Using a recipe of basic and advanced search features can greatly narrow the number of results returned and give you better data. Instead of searching for Name of Financial Institution, use "Name of Financial Institution" in quotations or narrow your results with more details like "Name of Financial Institution" "Confidential Handling" to find any leaked company documents with "confidential handling" in the metadata or headers. Check out Google advanced search or search for "Google Hack Lists" for more tricks like finding the bank's IP CCTV cameras and password lists.

Google Alerts. Once you have narrowed your search and tested it out, use Google Alerts (www.google.com/alerts) to have Google e-mail you anytime the search criteria is found by Google's extensive web crawlers.

Network Management Issues regarding Social Media Sites:

- Consider monitoring traffic that goes to social networking sites using intrusion detection services. Signatures can be written that report traffic to social networking sites.
- Consider setting up separate v-lan for surfing out to the social networking sites.
- Determine whether content filters should be configured to prohibit visiting social media sites.

Note: Appendix D is meant for larger banks where IT personnel are sent into the field regularly and may witness actions that warrant reporting. Rarely do smaller banks adopt this.

Appendix D: Potential Incident Report

☐ **CHECK HERE IF DISCLOSURE INCIDENT**

Date: _____

Name: _____ Title: _____

Location of Incident: _____
Person(s) Involved in Incident: _____
_____

Description of Incident: _____
_____
_____
_____
_____
_____
_____
_____

Please attach supporting documentation.

ISO Use Only Date of Receipt: _____

Initial Severity Level Assignment: _____

[Computer Incident Response Team / IRT] Submission Date: _____

[Computer Incident Response Team / IRT] Review Summary:

_____
_____
_____
_____
_____
_____
_____

Response to Incident: _____
_____
_____

The Incident Response Plan

- Components of a Good Plan
- Reporting Requirements
- Training Considerations

PIR's (Appendix A)

- For larger banks.
- Still, may make good training material for the IRT.
- We don't have time to review in this workshop.

infotex

Incident Logs

- If you use for one incident, you need to use for all security incidents!
- Lays a paper trail over time for an incident.
- Most may not be finished.

infotex

Incident Response Plan

- **Show 'em reference in the plan (page 19), then Appendix A (page 26.)**
- **Show them the Incident Log**

infotex

See Incident Response As . . .

Incident Reporting

- Broadcast Awareness (Real Time)
- Incident Log
- Notification
  - Executive Management
  - Board of Directors
  - Customers
  - Examiners, Law Enforcement
- Summary Reports
- Annual Report to the Board

infotex

Simplify IT

- Five Types of Incident Reporting
  1. Broadcast Awareness (Real Time)
  2. Incident Log
  3. Notification
  4. Summary Reports
  5. Annual Report to the Board

infotex

Self Reporting

- When somebody clicks on a link, what do you want them to do?
- When you receive the results of an audit report, what do you do?

infotex

Reporting Techniques

- The more you integrate Customer Awareness Training into everything your bank does, the better off you'll be in an incident.

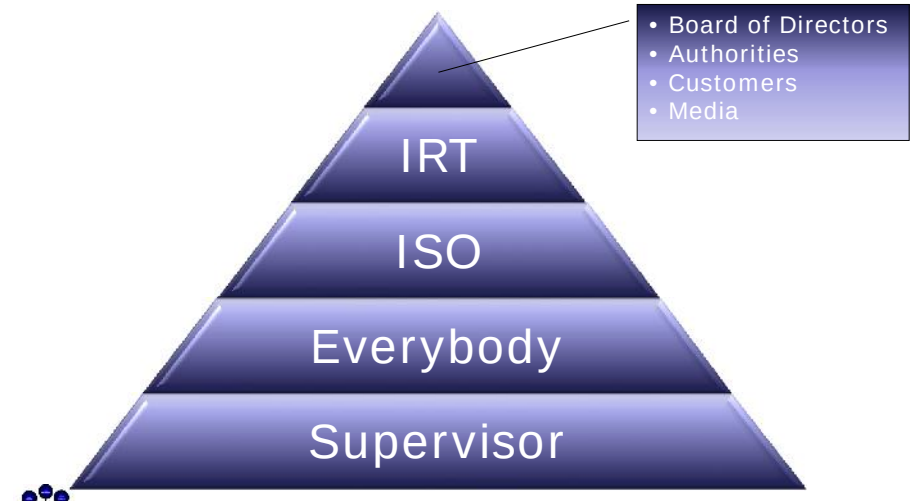
infotex

Reporting Techniques

- Must include training in Security Awareness Training on how to report suspicious activity!
- We call it "Broadcast Awareness."

infotex

Broadcast Awareness



infotex

Annual Report to the Board

- FFIEC Guidelines require that the ISO's Annual Report to the Board include a summary of "security events."
- We believe this would go beyond notification incidents, and include high severity security and the stats on negative incidents as well.

infotex

Annual Report to the Board

- This responsibility does not preclude real-time reporting of high severity events.
- This can be “broken out” of other ISO reporting requirements or included all in one report.

infotex

Annual Report to the Board

- **Show ‘em the actual word document!**

infotex

Who else receives "reports?"

- IRT
- Media
- Law Enforcement
- Customers

infotex

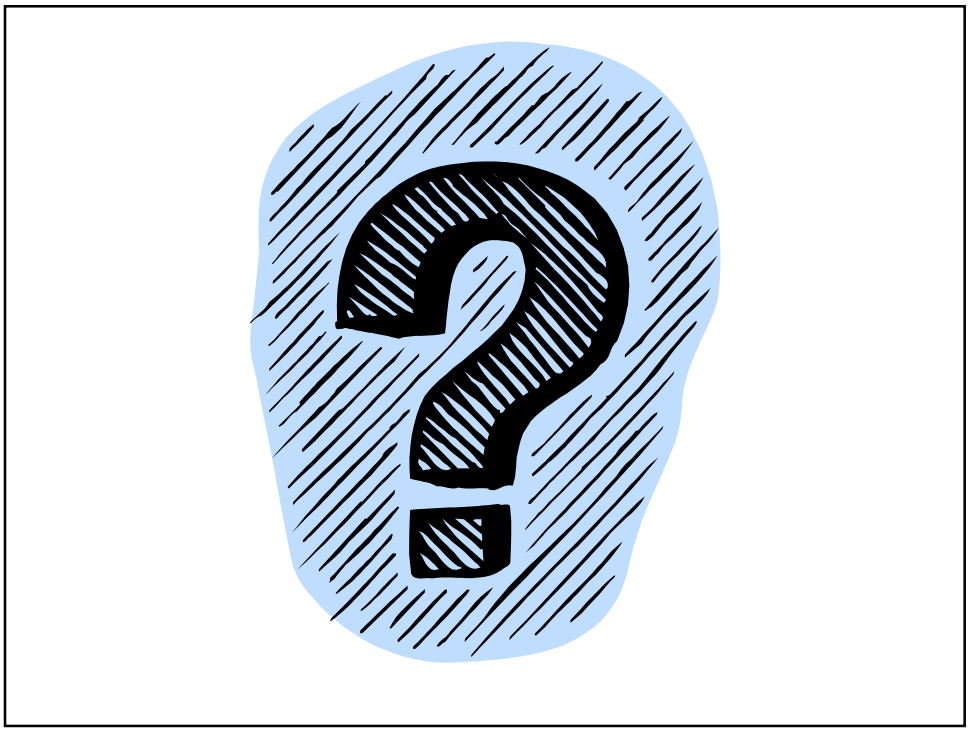
Pro-active Re-active Goals

CAT
- Ruthless Integration

Broadcast Awareness
- Involve Customers and Media

Media Relations
- DRP, BCP, Community

infotex



Team & Reporting

Exercise!

Mini-Quiz #1

infotex

Incident Response Team: Who is / should be on your Incident Response Team?

1) _____ 6) _____
2) _____ 7) _____
3) _____ 8) _____
4) _____ 9) _____
5) _____ 10) _____

Typical members (in a community-based financial institution): IS Steering Committee / Teller / Branch Manager / Loan Officer / Human Resources / Network Administrators and other technical people not on the Steering Committee / Marketing / Accounting or Finance / President or Executive Management / Legal

Open Book: Pleae use your handout and notes if you wish!

Incident Reporting: What are the four types of Incident Reporting?

1) _____
2) **Incident Logging:** How we document the incident as it unfolds.
3) _____
4) _____
5) _____

Broadcast Awareness: What are the five phases of Broadcast Awareness?

1) **Broadcast Awareness:** Get with your supervisor
2) **Everybody:** Then make all appropriate entities are aware of the potential incident ASAP.
3) _____
4) _____
5) _____

Annual Report to the Board: Which of the following types of incidents should be included in the Annual Report to the Board?

Notification Incidents Security Incidents Negative Incidents

The Incident Response Plan

- Components of a Good Plan
- Reporting Requirements
- Training Considerations

Training Objectives

1. Why you're on the team
   - Why multi-disciplinary
   - Roles, responsibilities
2. The Incident Response Policy
   - Incident Classification
   - What constitutes a "notification incident"

Training Objectives

3. The Team Meetings
   - Try to restrict work to team meetings.
   - Agendas
   - Review Reports
   - Read Minutes (and meet commitments agreed to as documented in minutes.)

Training Objectives

4. The Incident Response Plan
   - Broadcast Awareness Procedures
   - Triage Process (event classification)
   - Priorities, Process, Objectives

Training Objectives

5. Response Tools
   - Decision Trees, Calling Trees
   - Talking Points
   - The Letter (which could be an e-mail, radio announcement, Facebook post, etc.)

Let's see what these can look like!

Quick!

Reading Time!

IRT Comprehension Exercise

infotex

What are the first three things we should do when we have an incident?

1) _____

2) _____

3) _____

Triage

What are the three steps that should be taken to determine whether we should notify our customers of a (potential) incident?

1) _____

2) _____

   A. Has misuse occurred?
   B. Is there a potential that misuse can occur? (ie: we don't know who has access to the data.)

3) Respond: Classify, Document, Escalate!

Classifications

What are the three classifications of an incident?

1) _____

2) _____

3) _____

Four Steps of Incident Response

What are the four steps of Incident Response according to NIST?

1) _____

2) _____

3) _____

4) _____

What are the first three things we should do when we have an incident?

1) Broadcast Awareness (as per Acceptable Use Policy and User Awareness Training)

2) Notify the Information Security Officer

3) Assist in the Triage Process

Customer Disclosure Requirements

What are the three steps that should be taken to determine whether we should notify our customers of a (potential) incident?

1) Detect the incident or Broadcast Awareness is acceptable.

2) Assess the scope: was there, or could there be, unauthorized access to customer information?

   A. Has misuse occurred?
   B. Is there a potential that misuse can occur? (ie: we don't know who has access to the data.)

3) Respond: Classify, Document, Escalate!

Classsifications

What are the three classifications of an incident?

1) Disclosure Incident

2) Security Incident

3) Negative Incident

Four Steps of Incident Response

What are the four steps of Incident Response according to NIST?

1) Prepare

2) Detect and Respond

3) Contain, Eradicate, Recover

4) Post-incident Review

Two Primary Tests

- Plan Walkthrough (before/during annual update)
- Tabletop Test (in addition, at least annual)

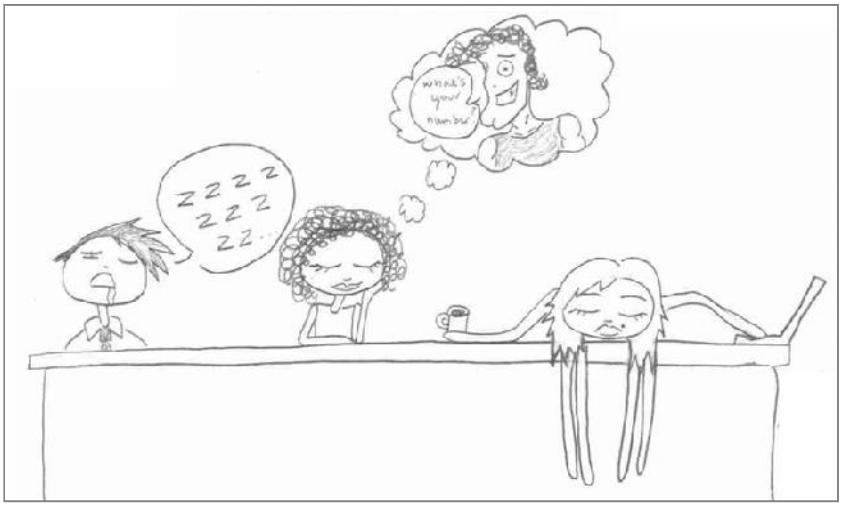
Additional Tests

- Functional – Think twice , Get Maalox Credit
- Audit – feed social engineering results into IRT Agenda and Minutes. Work with auditor to time Broadcast Awareness.
- Exercises: Clean desktop, EICAR??

Post-Mortem Reviews

- No, you don't have to call them that. (NIST calls them Post-Incident Activity)
- Should be conducted after every critical incident (plan should specify what type of incident).
- Should be conducted after every test.
- Can be used to make a real event a "Maalox Test."
- Mini-Quiz Three has some examples.

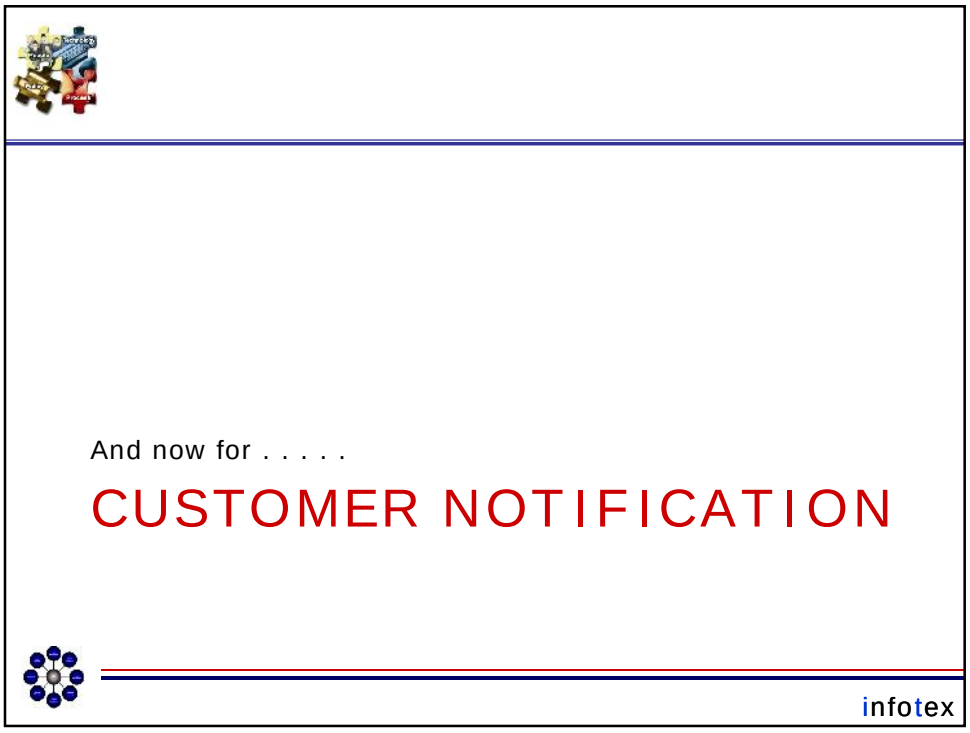
Do we need a break?

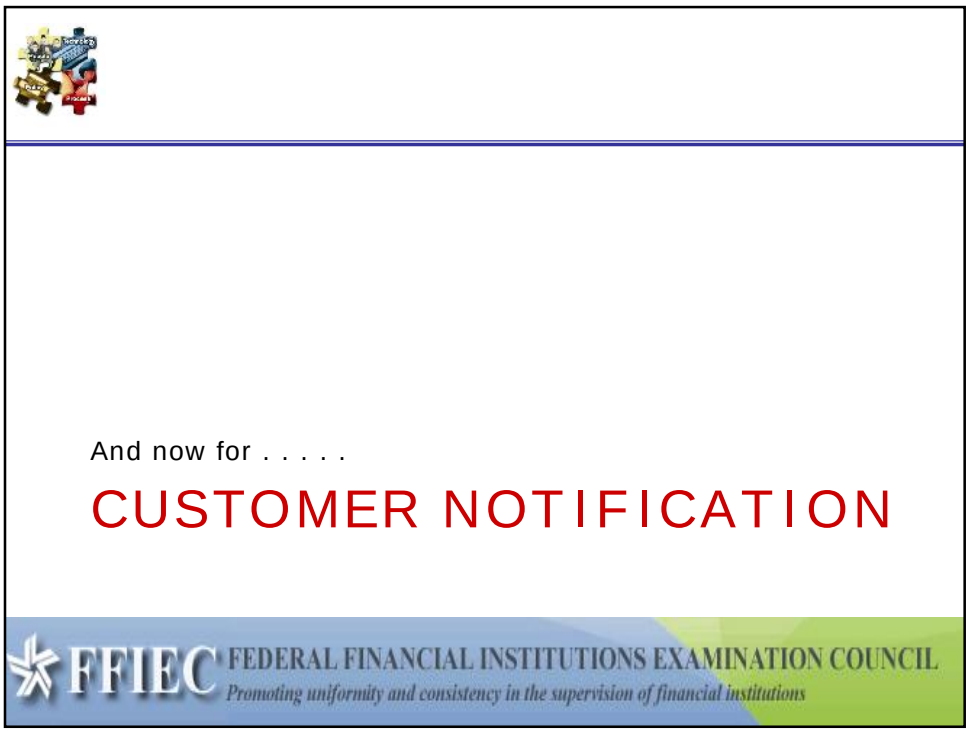


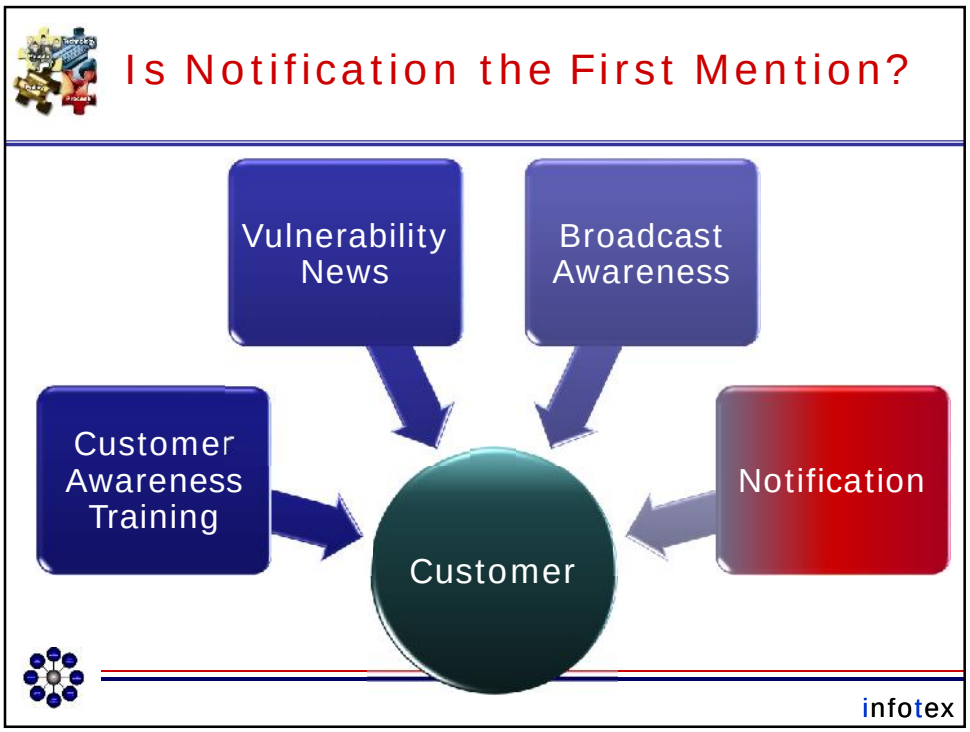
infotex

Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Framework
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!


And now for . . . . .
CUSTOMER NOTIFICATION
infotex


And now for . . . . .
CUSTOMER NOTIFICATION
FFIEC
FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions


Is Notification the First Mention?
Vulnerability News
Broadcast Awareness
Customer Awareness Training
Customer
Notification
infotex

FDIC Appendix B part 364

- Page 5: Response Program
- Page 6: Customer Notice
- Page 7: Content of Customer Notice

Let's see the regs!

And what does it do?

- Spells out a five step process for responding to customer information breaches.
- Defines "customer information."
- Defines when notification must occur.
- Specifies what should be in the customer notice.
- Addresses how to deliver the notice.

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

Remember FIL-27-2005

- Spells out a five step process for responding to customer information breaches.
- Defines "customer information."
- Defines when notification must occur.
- Specifies what should be in the customer notice.
- Addresses how to deliver the notice.

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

What the FDIC says . . .

- **Show 'em the actual PDF document!**

Let's see the regs!

The five steps . . .

1. Assess the nature and scope of the incident and identify what customer information systems and types of customer information have been accessed or misused;

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

The five steps . . .

2. Notify your primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

The five steps . . .

3. File a timely SAR, and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notify appropriate law enforcement authorities;

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

The five steps . . .

4. Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

The five steps . . .

5. Notify customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it.

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

Simplify IT

- The FDIC 5 Steps for Notification
  1. Triage: Assess nature and scope of incident and determine if customer notification is required. (Determine Disclosure Requirements)
  2. Notify your federal regulator.
  3. File a timely SAR.
  4. Contain and Control
  5. Notify Customer

infotex

Customer Information

- A customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number,
- or a personal identification number or password that would permit access to the customer's account.

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

Customer Information

- The FFIEC's definition also includes any combination of components of customer information that would allow someone to log on to or access the customer's account, such as user name and password or password and account number.

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

When?

- "a financial institution should provide a notice to its customers whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur.

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

When: Let's break that down.

1. whenever it (the bank) becomes aware of an incident
2. of unauthorized access to customer information and,
3. at the conclusion of a reasonable investigation,
4. determines that misuse of the information has occurred
5. or it is reasonably possible that misuse will occur.

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

Simplify IT

- Triage: Determining Disclosure Requirements
  1. Detect: Broadcast Awareness
  2. Assess: Real or potential unauthorized access to customer data? Who, what, when, how, where?
  3. Respond: Classify, Document, and Escalate! (A reasonable investigation means documentation and escalation!)
     A. Has misuse occurred?
     B. Or is there a potential that misuse could occur?

infotex

Potential for Misuse

- Lost or stolen laptop that's unencrypted.
- E-mail sent in the clear.
  - Check the route, sometimes no hops!
- Smart phone traded in to carrier without sanitization.
- Et cetera!

infotex

How

- "should be given in a clear and conspicuous manner."
- "Describe the incident;
- Type of information subject to unauthorized access;
- Measures taken by the institution to protect customers from further unauthorized access;

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

How

- Telephone number customers can call for information and assistance; and
- Remind customers to remain vigilant over next twelve to twenty four months, and
- report suspected identity theft incidents to the institution.

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

Customer Notification

- Notification Methods
  - E-mail
  - Telephone, Facsimile
  - Letter
- Broadcast Awareness Methods
  - Website
  - E-mail
  - Social Media
  - Media

infotex

Customer Notification

- Talking Points
  - For Employees
  - For Management
  - For ISO
  - For Media Contact

infotex

Notification Message

- Do start the message out looking like it's a marketing piece about how you want to protect customer information.
- Do be unconcerned if the message turns out to be more than one page long.

infotex

Notification Message

- Do be sure to stress that your bank does everything possible to prevent information security breaches.
- Do be sure to point out that no matter what you can do, there is no such thing as 100% security.

infotex

Notification Message

- Describe the incident as briefly as possible.
  - Do NOT quote the law that is requiring you to send the message.
  - Do NOT come off like you are trying to blame somebody.

infotex

Notification Message

- Describe the incident as briefly as possible.
  - Include the date of the incident.
  - Include what information was breached.
    - Use “might have been” if possible.
  - Do NOT include how many persons were affected if possible.
  - Do NOT include what caused the breach.

infotex

Notification Message

- Do include credit bureau information so that customers can put a watch on their credit.
- Do include brochures about identity theft protection.

infotex

Notification Message

- Do put a contact number and make sure all employees know to funnel information requests to this number.
- Do be prepared for calls from customers as well as media.

infotex

Notification Message

- Do share your regrets and apologize.
  - You won't be sued for being sorry that an action occurred.
  - You MIGHT get sued if you don't come off as sorry.
- Do have the highest level signature you can muster up.
  - (Preferably President or CEO)

infotex

Transparency Synonyms

- Truthfulness
- Completeness
- Accuracy
- Timeliness
- Smartness

infotex

While in training . . . .

- Consider playing this video, with sound down, while you talk to your Incident Response Team about the meaning of, and the need for, transparency.
- https://www.youtube.com/watch?v=jvgBWzRjUIU

infotex

m.infotex.com/dripdrip

infotex

Before it's too late!

- Meet the lawyer that will be called when the going gets tough.
- Make sure your lawyer understands the need to comply with federal regulations (and avoid state).
- Play that Target Video for your lawyer!

infotex

Tools

Reading Time!

Customer Notification Letter

infotex

<Name of Financial Institution> is committed to maintaining the privacy of our customer's information. We do everything possible to protect customer information, and are audited and examined by regulators regularly to ensure that we keep up with the latest technologies, processes, and procedures necessary to prevent an incident from occurring. However, there is no such thing as 100% security. We have many provisions in place to protect your information, but there is always a potential for failure. We are writing to inform you of a recent security incident at **<Name of Financial Institution>**.

[Describe the incident as briefly as possible, including the date of the incident, what information was breached, and what you have done to contain the breach. You do NOT need to include how many persons were breached, nor do you need to include who caused the breach. Consider "TMI."] We have taken steps to contact all associated individuals in order to mitigate the impact of this breach.

We regret that your information may have been subject to unauthorized access and have taken remedial measures to ensure that this situation is not repeated. Although there is no evidence that an unauthorized individual has obtained your personal data, w / W]e are bringing the incident to your attention so that you can take precautions along with our efforts to minimize or eliminate any potential misuse of your personal identity.

To protect yourself from the possibility of identity theft, you may place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call any one of the three credit reporting agencies at the phone numbers listed below. You should request that a fraud alert be placed on your account and order a free credit report from the agency.

Equifax	1-888-766-0008
Experian	1-888-397-3742
Trans Union	1-800-680-7289

When you receive your credit reports, review them carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report. If you find any suspicious activity on your credit reports, call your local police or sheriff's office.

Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in reviewing your credit reports from the three major credit reporting agencies. You may obtain a free copy of your credit report once every 12 months by visiting **www.annualcreditreport.com**, calling toll-free 877-322-8228 or by completing and mailing an Annual Credit Request Form which can be obtained from **www.ftc.gov/bcp/menus/consumer/credit/rights.shtm**.

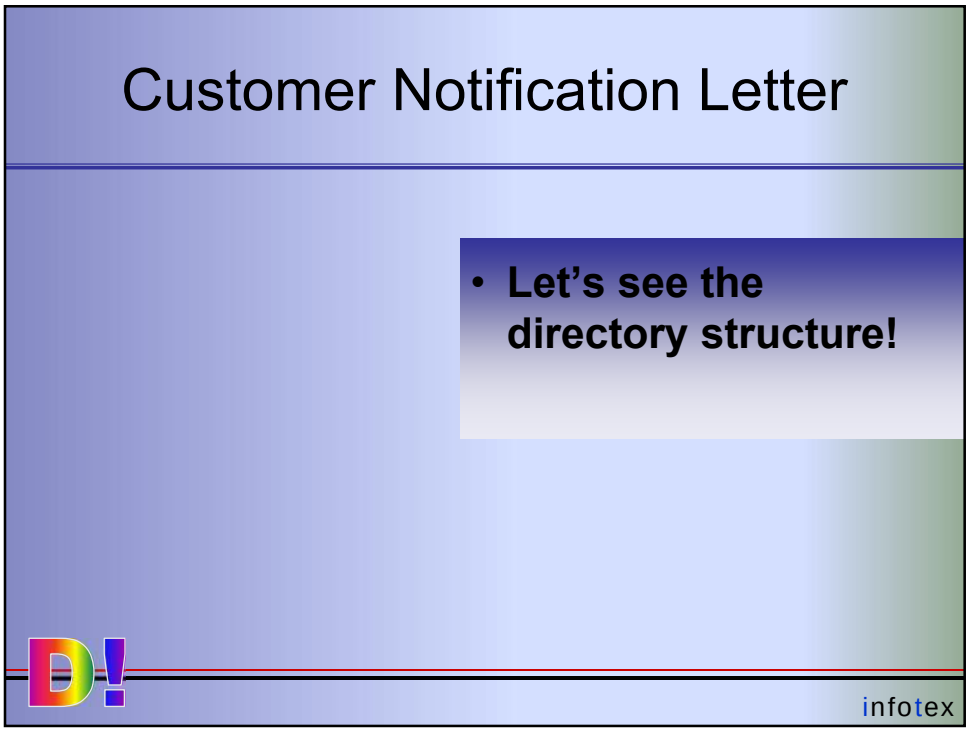
For more information on identity theft, you can visit the following websites:

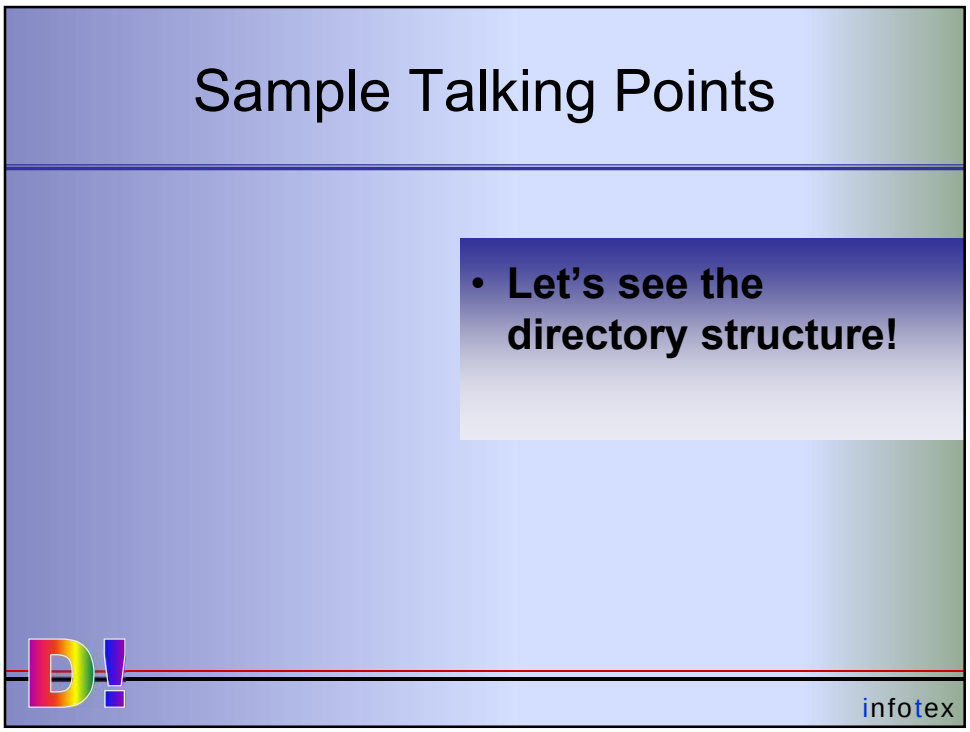
Indiana Attorney General at: **www.in.gov/attorneygeneral/2413.htm**
Federal Trade Commission at: **www.ftc.gov/bcp/edu/microsites/idtheft/**

Because **[Name of Financial Institution]** is so committed to maintaining the privacy of our customer's information, we sincerely regret any inconvenience this incident may have caused. Should you have further questions about this matter, please contact [Name / Title] at [e-mail address] or call at [phone number].

Sincerely,

[Name]
President
[Name of Financial Institution]


Customer Notification Letter
• Let's see the directory structure!
infotex


Sample Talking Points
• Let's see the directory structure!
infotex

Engaging the Media

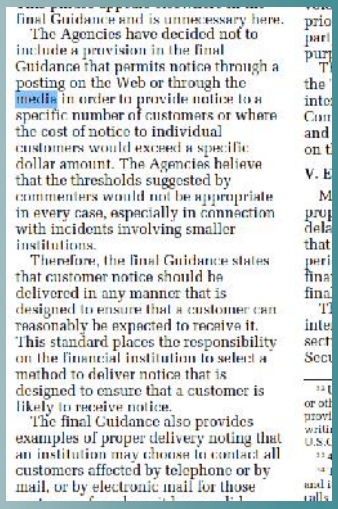
- Though not really a "reporting requirement" this is still an extremely important part of any Incident Response Plan.
- Let's focus on the customer first, knowing that notifying the customer is the BEST WAY to notify the media.

infotex

Not a lot of . . . .

Advice from the Regs

- NIST SP800-61
  search for 2.3.4.1



final Guidance and is unnecessary here.
The Agencies have decided not to include a provision in the final Guidance that permits notice through a posting on the Web or through the media in order to provide notice to a specific number of customers or where the cost of notice to individual customers would exceed a specific dollar amount. The Agencies believe that the thresholds suggested by commenters would not be appropriate in every case, especially in connection with incidents involving smaller institutions.
Therefore, the final Guidance states that customer notice should be delivered in any manner that is designed to ensure that a customer can reasonably be expected to receive it. This standard places the responsibility on the financial institution to select a method to deliver notice that is designed to ensure that a customer is likely to receive notice.
The final Guidance also provides examples of proper delivery noting that an institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those

Interagency Guidelines

Basic Fundamentals

- "No comment" is a bad comment.
- Be prepared.
- NEVER EVER LIE.
- Share only what you know.
  - Saying "I don't know" is the way to go.
- But then get back to them!
- ALWAYS, ALWAYS, TELL THE TRUTH.

infotex

Get some training!

- http://mediaworksgroup.com/
- http://ragantraining.com/
- http://www.prsa.org
- http://www.businesstrainingworks.com

infotex

Engaging the Media

- Five Goals
  1. Start Early: Don't wait for an incident.
  2. Have a generic strategy (possibly in your plan).
  3. Have a specific strategy (customized to the incident).
  4. Choose the right person for the job.
  5. Create a "media reader" for that person.

infotex

1. Start Early

- Two causes:
  - Broadcast Awareness
  - Customer Notifications
- If you involve the media in broadcast awareness, you will have an easier time during customer notifications.

infotex

2. Have a generic strategy

- You should ALWAYS have a generic media strategy, including:
  - Who are you going to contact if you need to contact somebody?
  - What basic points should be expressed in any media contact (see your plan)!
  - When would you want to contact the media before they find out?

infotex

3. Have a specific strategy

- Before it's too late, create a written strategy for this specific incident:
  - Sometimes that can be hoping they don't find out, but preparing for if they do!
  - Other times, you might be better off contacting them in advance.

infotex

4. Choose the right person

- Who is your outgoing person?
- Who wanted to be a radio personality?
- Sometimes your President or CEO or even your marketing person is not the right person.
- Often your ISO is not the right person.

infotex

5. Create a Media Reader

- Finally, when you know the media is calling (and you should always set it up so that you know the media is calling), or before an interview, have a set of “talking points” or what we call “media readers” that you read in advance of the talk, to calm your nerves and remind you of your strategy.

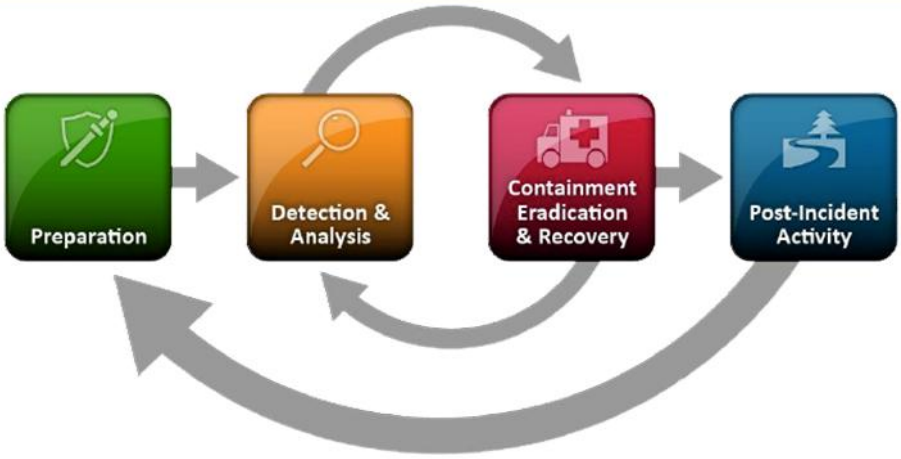
infotex

Simplify IT

- Engaging the Media
  1. Start Early
  2. Pre-train on a “generic strategy”
  3. Use the “generic strategy” to document a strategy specific to the incident, get IRT approval
  4. Choose the right person to speak to the media.
  5. Create a “media reader”

infotex

NIST Response Cycle



infotex

Simplify IT

- The NIST Incident Response Cycle
  1. Prepare
  2. Detect and Analyze
  3. Contain, Eradicate, Recover
  4. Post-Incident Review

infotex

Media Readers

- **Let's see the directory structure!**

infotex

First, some questions . . .

FFIEC Incident Response Testing Requirements

What three "documents" should accompany every Disaster Recovery (and thus, we suspect, every Incident Response) Test?

1) Test Plan
2) _____
3) _____

Triage Process

What are the three steps of Triage?

1) Detect
2) _____
3) _____

Process of Customer Notification

What are the five steps the FFIEC requires we use when it comes to "disclosure incidents?" (Hint: see the policy boilerplate!)

1) _____
2) Notify your federal regulator (as if we're going to do this before we contain the incident!)
3) _____
4) _____
5) _____

Next, the Incident Reponse Test Plan . . .

Test Plan

Date: 06/04/15

Attendees:

- Dan Hadaway; CRISC, CISA, CISM; Infotex . . . . . Test Facilitator
- _____ (print your name)

Test Process:

Infotex will lead us through the testing of the scenarios defined below, using the following process:

- Propose Test Plan / Test Plan Approval (already completed, this document is the deliverable)
- Test Plan Communication (requires attendance of Incident Response Team, which for today will be you and your imagination!)
- Test (conducted against the above defined Incident Response Team on 06/04/15)
- Post-mortem Analysis (performed on 06/04/15)
- Final Report (which you'll have to do when you get home and apply this to your team)

Testing Method:

Simulation (Tabletop) Test: A tabletop test is somewhat more involved than an walk-through because the participants choose a specific event scenario and applies the Incident Response Plan to it:

- Practice and validation of specific functional response capability based on specific scenarios;
- Focus on demonstration of knowledge and skills, as well as team interaction and decision-making capability;
- Role playing with simulated response at alternate locations/facilities to act out critical steps, recognize difficulties, and resolve problems in a non-threatening environment;
- Mobilization of all or some of the crisis management/response team to practice proper coordination; and
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization to reinforce the content and logic of the plan.

Emergency Scenarios:

Accidental Leak of Data: There will be 2 different scenarios, each of which will be tested and documented separately. Details of each test will not be delivered to the Incident Response Team (IRT) until just prior to each test scenario.

What should you bring?

All you need to bring to the test is your copy of the Incident Response Plan, as well as some paper and something to write with! If you are 100% certain you would have your smart phone during any type of an incident, you are welcome to bring it along as a resource.

Test Rules:

- We must limit outside interruptions unless they are part of the test.
- Infotex will bring different examples within the test scenarios defined above.
- The team has to accept the facts described in each scenario.
- Everyone has equal right to contribute.
- Silence is acceptance / agreement.
- Only Infotex is allowed to "call timeout" but you can appeal to the Infotex consultant to do so.

Evaluation Criteria:

- Was the organization's Incident Response Policy enforced?
- Do participants understand the organization of the plan?
- Are responsibilities correctly assigned?
- Can responsibilities be carried out successfully?
- Are procedures clear? (Were there instances of confusion?)
- Are procedures complete? (Should additional tasks be documented?)
- Does the plan facilitate all necessary communication?
- Were plan objectives (RTOs, etc.) met?

Additional Dates:

06/04/15: Test Plan Review
06/04/15: Test Day
06/04/15: Post Mortem Review.

TEST DAY DOCUMENTATION:

Date: 06/04/15

Attendees:

- Dan Hadaway; CRISC, CISA, CISM; Infotex . . . . . Test Facilitator
- _____ (print your name)

Test Scenario: Accidental Data Leakage

Scenario One:

A loan officer from Branch One has a habit of taking her laptop home every weekend. At 3:30pm on Sunday afternoon, she left a message on the Information Security Officer's phone that her house had been robbed, and that she thinks her laptop was taken with the rest of her belongings. At 3:40, the Information Security Officer discovers that voice mail.

Detecton and Analysis:

What questions will you ask when you return her call?
What questions do you need to ask IT in order to determine impact?
What are your immediate top priorities?

So the loan officer, whose name is Suzie, says that she did have several loan files on her computer, and that she was storing them on the "S" Drive where IT told her to store them. But she can't remember if the laptop was powered on or off. She swears that she keeps it locked even when she is not at home. You contacted IT, and discovered that the S drive is indeed the encrypted drive. IT also says that they have never seen her laptop left unlocked in her office. IT confirms that auto-lock policy is enabled on the laptop.

Contain and Eradicate:

Has the incident been contained? When?

What are the known impacts?
What are the potential impacts?
Who needs to be involved?
Who needs to be notified?
What would you instruct Suzie to do now?
What should IT be doing now?

Do you have enough information to "classify" this incident?
How would you classify it?

What are the next steps, having made that classification?

What other questions should be asked?

Test Scenario One: Accidental Data Leakage

Sub-Scenario Two:

A loan officer from Branch One has a habit of taking her laptop home every weekend. At 3:30pm on Sunday afternoon, she left a message on the Information Security Officer's phone that her house had been robbed, and that she thinks her laptop was taken with the rest of her belongings. At 3:40, the Information Security Officer discovers that voice mail.

Detecton and Analysis:

What questions will you ask when you return her call?
What questions do you need to ask IT in order to determine impact?
What are your immediate top priorities?

So the loan officer, whose name is Suzie, says that she did have several loan files on her computer, and that she was storing them on the "S" Drive where IT told her to store them. But she can't remember if the laptop was powered on or off. When you asked if she had locked it before she left she said, "huh?" When you explained she said that she though the laptop was auto-locked. You contacted IT, and discovered that the S drive is indeed the encrypted drive. But IT also says that they have been having some issues with that laptop and they think, can't be sure, but they think auto-lock may have been disabled on the laptop.

Contain and Eradicate:

Has the incident been contained? When?

What are the known impacts?
What are the potential impacts?
Who needs to be involved?
Who needs to be notified?
What would you instruct Suzie to do now?
What should IT be doing now?

Do you have enough information to "classify" this incident?
How would you classify it?

What are the next steps, having made that classification?

What other questions should be asked?

Surprise Scenario 2.5 (Black Swan):

Two weeks later law enforcement calls saying they found the laptop. You meet them and check and, sure enough, the S drive had been unencrypted. Moreover, the results of the last (very bad) OCC Examination were also on that S drive. And the loan officer? Turns out she might be involved with the person arrested by the police. And guess what, the ISO is on a cruise ship and can not be reached.

Contain and Eradicate:

Has the incident been contained? When?

What are the known impacts?
What are the potential impacts?
Who needs to be involved?
Who needs to be notified?
What would you instruct Suzie to do now?
What should IT be doing now?

Do you have enough information to "classify" this incident?
How would you classify it?

What are the next steps, having made that classification?

Given the loan officer's potential involvement wth the suspect, who else should be brought in to help?

What other questions should be asked?

Post-Mortem Review:

Attendees:

- Dan Hadaway; CRISC, CISA, CISM; Infotex . . . . . Test Facilitator
- _____ (print your name)

Test Scenario: Accidental Data Leakage

Scenario One:

Current classification of Incident:

How long did it take to broadcast awareness?
When was the incident contained?
How long did it take to contain the incident?

What were some issues that came out of the incident?

What did we do right?
What did we do wrong?
What questions do we wish we asked?
How could we have been more prepared?

What can be done to prevent the incident from happening again?

What action items are a result of this incident?

Should this incident be reported to the board?

What other questions should be asked?

Can we close this incident?

Scenario Two:

Current classification of Incident:

Records Involved:

Have all customers been notified?

Has anything been said by customers at the branch? Who is handling this? What is the status of this?

Is the media still interested? Who is handling this? What is the status of this?

How many customers have taken us up on our offer for credit monitoring?

What other metrics should we be tracking?

What were some issues that came out of the incident?

What did we do right?
What did we do wrong?
What questions do we wish we asked?
How could we have been more prepared?

What can be done to prevent the incident from happening again?

How long did it take to broadcast awareness?
When was the incident contained?
How long did it take to contain the incident?

What action items are a result of this incident?

Should this incident be reported to the board?

What other questions should be asked?

Can we close this incident?

Scenario Two Point Five:

Current classification of Incident:

Records Involved:

Have all customers been notified?

Has anything been said by customers at the branch? Who is handling this? What is the status of this?

Is the media still interested? Who is handling this? What is the status of this?

How many customers have taken us up on our offer for credit monitoring?

What other metrics should we be tracking?

Who what why and when on the loan officer's involvement with the

What were some issues that came out of the incident?

What did we do right?
What did we do wrong?
What questions do we wish we asked?
How could we have been more prepared?

What can be done to prevent the incident from happening again?

How long did it take to broadcast awareness?
When was the incident contained?
How long did it take to contain the incident?

What action items are a result of this incident?

Should this incident be reported to the board?

What other questions should be asked?

Can we close this incident?

Aren't we glad we notified our customers even though we weren't 100% sure if it was truly a breach or not???

Disclosure Incidents

Tips for IRT Testing

- Attendance is critical.
- Simulate reality, but try to use imagination.
- Set realistic goals and objectives
- Simulate decision making under normal and then stressful conditions
- Have surprise elements, try a black swan version of the test.
- Provide room for participants to make errors and learn from them

infotex

Scenario Descriptions

- Lost BYOD
- DDoS Attack
- ATM Cash-Out
- Laptop/Mobile Device Loss
- Destructive Malware
- Third-Party Breach
- Internal Fraud
- Accidental Disclosure
- ATM Skimming
- Inappropriate Use
- Rogue Employee
- Compromised Credentials

infotex 2

Two New Statements

- FFIEC Statement on Destructive Malware
  - Bottom of page 2
- FFIEC Statement on Compromised Credentials
  - Monitoring in middle of page 3

Let's see the regs!

Law Enforcement

- Most bankers are disappointed with their experience trying to enlist law enforcement.
- Still, they want your input and they want to reach out to you.
- Cooperating will only put you in a better position during a “crisis.”

infotex

Yet, right here in Indiana

The FBI’s “Cyber Crime Unit” is right here in Indiana.

Contact: Jim Kunkel
James.Kunkel@ic.fbi.gov

infotex

Call us if you have an incident!

- The Secret Service:

Gary L. Durham
Special Agent in Charge
U.S. Secret Service
Indianapolis Field Office
317-822-5001 Direct Line
317-315-0656 Cell

infotex

Law Enforcement

- Private companies fill the void . . .
- Phishing Site Take-downs
  - Netcraft (www.netcraft.com)
  - MarkMonitor (www.markmonitor.com)
  - FraudWatch (www.fraudwatchinternational.com)

infotex

Law Enforcement

- Private companies fill the void . . .
- Digital Forensics / Digital Discovery
  - Packet Ninjas (www.packetninjas.net)
  - infotex: (www.infotex.com)
  - Data Chasers: (http://www.datachaserscomputerforensics.com)

infotex

Notifying your Examiner

- Like the media and law enforcement, the more you involve your examiners in “broadcast awareness,” the better position you’ll be in during a “crisis.”
- As per FIL-27-2005, you are required to notify your examiners in “disclosure incidents.”

infotex

Go above and beyond!

- As a rule, no surprises.
- Definitely notify your examiner of a "disclosure incident."
- Anything that you would report to your board, consider notifying your examiner in real time.
- They'll find out anyway!

infotex

Decision Tree

- In practice, it's more of a pro-active training tool than a live situation reaction tool.
- Still, it should be kept up-to-date and reviewed at least annually.
- One time to update it is when you're performing your risk assessments.

infotex

Decision Tree

- IDS vs. ELM vs. PIR Incidents
- Keep Incident Categories Simple
- Immediate Reaction
- Reporting to Board
  - Size of bank seems to impact board reporting
  - Be sure to equalize with your Impact Severity Procedure
- Follow-up Duties

infotex

Identifying Potential Incidents

- Incident Response Team Meetings
- Risk Assessments
- Drill-down Risk Assessments
- Audits, Examinations, Workshops

infotex

Incident Response Plan - Decision Tree

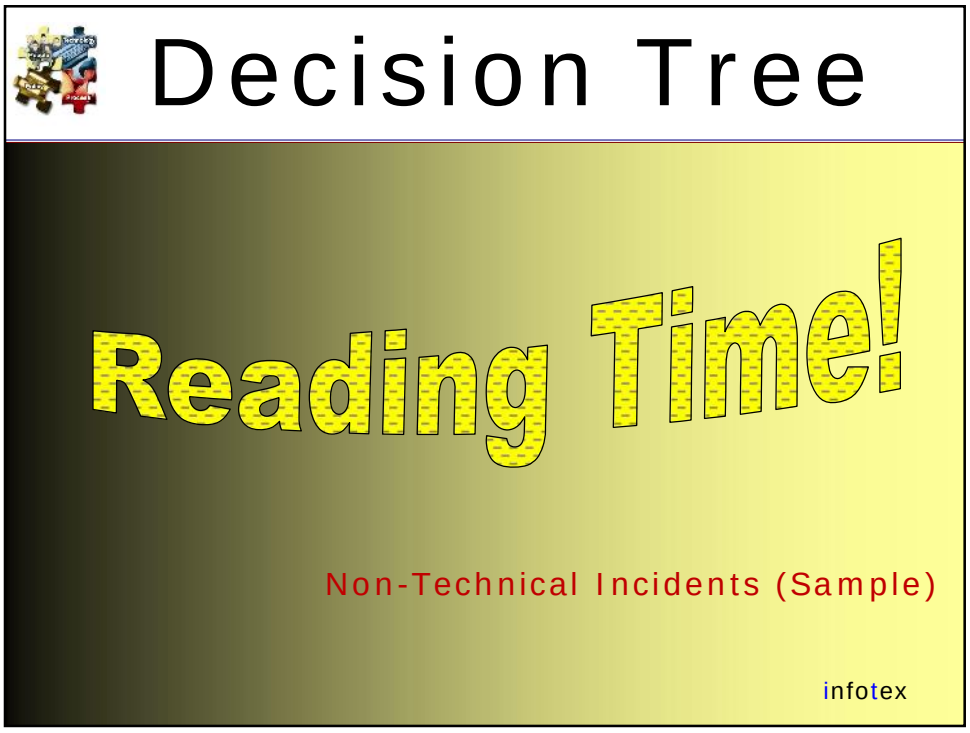
(P24) / Cobit Processes: PO9, DS8, DS10, ME2

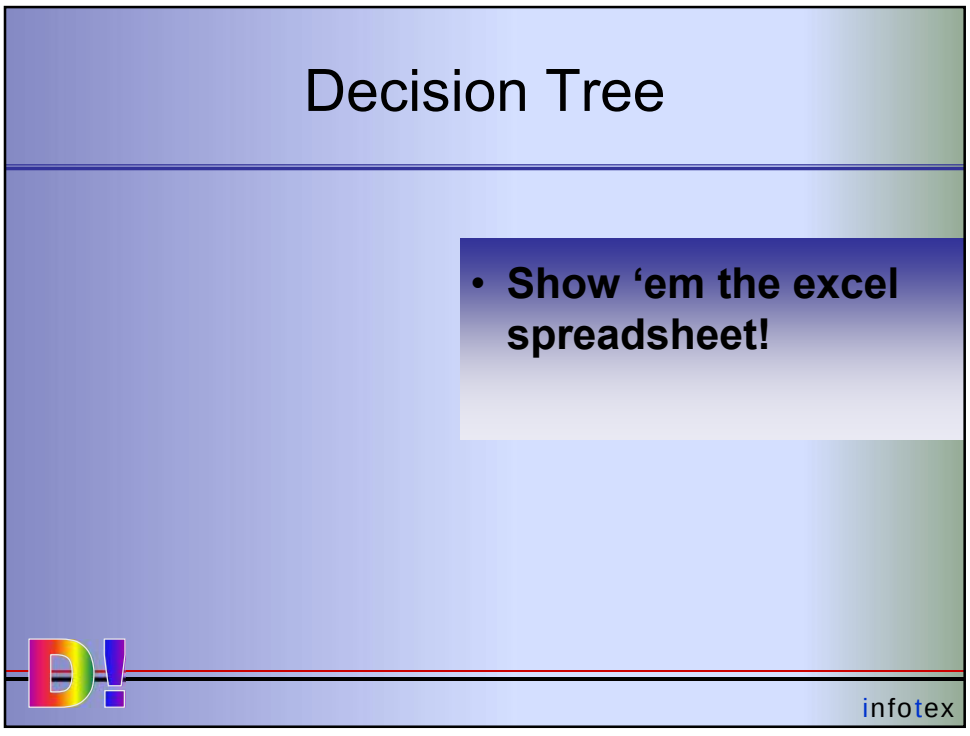
Plan Owner:
Plan Reviewers:

Date: _____

	Incident Category	Type	Immediate Reaction	Immediate Notification	Follow-up Duties	Min Severity Rating	PIR Required?	Report to Board?	Call Emergency CIRT Meeting
40	Physical Breach Attempt	Malicious	Notify all other locations immediately	All Location Shift Managers	Investigate Source, Follow-up Report in next CIRT meeting	3	Y	Y	Y
41	Employee E-mails (or otherwise sends) data to the wrong person.	Data Leakage	Determine volume, if over X call Emergency CIRT.	Call ISO.	Determine if Customer Notification is warranted. If so, call Emergency CIRT.	2	N	Y	Y
42	DDoS Attack	Malicious	Execute DDoS Response Procedure.	Call Emergency CIRT Meeting	Follow DDoS Response Procedure	2	N	Y	Y
43	Corporate Account Takeover	Malicious	Execute CATO Response Procedure	Call Emergency CIRT Meeting	Follow CATO Respone Procedure	1	N	Y	Y
44	Rogue USB Sticks	Malicious	Disconnect device it was plugged into, implement anti-virus procedures.	Call Help Desk, call all locations, inform ISO.	Follow virus removal procedure, perform forensics analysis to determine extent of any damage.	2	Y	Y	Y
45	Telephone Social Engineering Attempt	Malicious	E-mail all employees and call all locations	E-mail all employees and call all locations	Investigate Source, Follow-up Report in next CIRT meeting	3	Y	Y	Y
46	Phishing Attempt (on the Organization)	Malicious	E-mail all employees and call all locations	E-mail all employees and call all locations	Investigate Source, Follow-up Report in next CIRT meeting	3	Y	Y	Y
47	Phishing Attempt (on general public)	Malicious	E-mail all employees and call all locations	E-mail all employees and call all locations	Investigate Source, Follow-up Report in next CIRT meeting	3	Y	Y	Y
48	Malware (not detected by technical controls)	Malicious	1) Contain and Eradicate the attack. 2) Notify ISO	E-mail ISO	Contain and Eradicate Virus, Investigate DAT Updating Configuration, Follow-up Report in next CIRT Meeting.	2	N	N	maybe
49	Unlocked Workstations found	Policy Violation	Confront Employee if possible, Notify ISO	Email ISO	ISO e-mails Security Reminder	NA	N	N	N
50	Written passwords found	Policy Violation	Confront Employee if possible, Notify ISO	Email ISO	ISO e-mails Security Reminder	NA	N	N	N
51	Forwarded Jokes, E-chain Letters, etc.	Policy Violation	Confront Employee if possible, Notify ISO	Email ISO	ISO e-mails Security Reminder	NA	N	N	N
52	Employee observed with a prohibited device (such as a USB drive or iPod connected to workstation.)	Policy Violation	1) Confront the individual and confirm authorization. 2) If not authorized, and employee does not share contents and remove from facility, contact security. 3) Notify HR via Email 4) Notify ISO	Email ISO and HR	Investigate Source, Follow-up Report in next CIRT meeting	1	N	N	N
53	Offensive/Illegal Files found	Policy Violation	1) Quarantine workstation 2) Notify ISO by Phone. 3) If ISO not available, notify employee's supervisor by phone. 4) E-mail Supervisor, HR and ISO. 5) File a PIR.	Notify ISO by phone	Investigate Source, Assign Severity Rating, Determine whether to Involve Law Enforcement, Follow-up Report in next CIRT meeting	4	Y	Y	Y
54	Unlicensed Software Found	Policy Violation	1) Decline to give access 2) Notify ISO via e-mail	Email ISO	Investigate Source, Follow-up Report in next CIRT meeting	varies	Y	N	maybe
55	Company Software installed at home	Policy Violation	Notify ISO	File PIR with ISO	Investigate Source, Follow-up Report in next CIRT meeting	3	Y	N	maybe
56	Other Improper Personal Use of Company Resources	Policy Violation	Notify ISO	File PIR with ISO	Investigate Source, Follow-up Report in next CIRT meeting	2	Y	N	N
57	Somebody is taking pictures in one of the locations	Suspicious Activity	1) Confront photographer 2) If no authorization, confiscate photography device 3) Notify ISO	E-mail ISO	Investigate Source, Follow-up Report in next CIRT meeting	varies	may be	N	N
58	Individual observed connecting a laptop or other device to the Organization's network that is NOT owned (and managed) by the Organization.	Suspicious Activity	1) Confront the individual and confirm authorization by calling and talking with supposed authorizer. 2) If not authorized, contact security. 3) Notify ISO	Verbally Notify Authorizer.	Follow-up report in next CIRT Meeting	varies	may be	N	N
59	Customer asks a question about our technology and we don't know the answer.	Technology	1) Send an e-mail to the Incident Response Team. 2) The ISO will determine whether to a) respond immediately with an answer b) call an emergency IRT meeting, or c) wait until a scheduled IRT meeting.	The ISO will respond immediately to the questioner and consider broadcasting awareness.	This will either be handled in real time or as part of a periodic meeting. The ISO will respond immediately to the person asking the question, and consider broadcasting awareness.	varies	N	N	maybe
60	A user discovers a problem with an application that requires immediate attention.	Technology	1) Send an e-mail to the Incident Response Team. 2) The ISO will determine whether to a) respond immediately with an answer b) call an emergency IRT meeting, or c) wait until a scheduled IRT meeting.	The ISO will respond immediately to the questioner and consider broadcasting awareness.	This will either be handled in real time or as part of a periodic meeting. The ISO will respond immediately to the person asking the question, and consider broadcasting awareness.	varies	N	N	maybe

	Incident Category	Type	Immediate Reaction	Immediate Notification	Follow-up Duties	Min Severity Rating	PIR Required?	Report to Board?	Call Emergency CIRT Meeting
61	A new technology, system, or device causes an unforeseen problem	Technology	1) Send an e-mail to the Incident Response Team. 2) The ISO will determine whether to a) respond immediately with an answer b) call an emergency IRT meeting, or c) wait until a scheduled IRT meeting.	The ISO will respond immediately to the questioner and consider broadcasting awareness.	This will either be handled in real time or as part of a periodic meeting. The ISO will respond immediately to the person asking the question, and consider broadcasting awareness.	varies	N	N	maybe
62	Stolen or Lost portable device (such as laptop, Smart Phone, iPad).	Potential	1) Notify ISO 2) Determine Severity Rating based on sensitivity of data stored on device. 3) Initiate Investigation 4) Involve Law Enforcement if necessary.	Notify ISO by phone	Investigate Source, Assign Severity Rating, Determine whether to Involve Law Enforcement, Follow-up Report in next CIRT meeting	4	Y	Y	Y
63	Stolen or lost backup tape, or any other medium with sensitive information.	Potential	1) Notify ISO 2) Determine Severity Rating based on sensitivity of data stored on device. 3) Initiate Investigation 4) Involve Law Enforcement if necessary.	Notify ISO by phone	Investigate Source, Assign Severity Rating, Determine whether to Involve Law Enforcement, Follow-up Report in next CIRT meeting	4	Y	Y	Y
64	A customer accuses us of leaking sensitive information, even if/when we did not leak the information	Potential	Notify ISO	Notify ISO by phone	Investigate Source, Follow-up Report in next CIRT meeting	2	N	N	N
65	A negative post is discovered on a Social Media site that has been posted by an employee.	Potential	Gather appropriate documentation (print-screens, dates, name of social media site, name of employee, how post was discovered). Notify Human Resources.	Notify Human Resources via e-mail.	Human Resources will consult with employee's supervisor and corrective action will be determined.	NA	N	N	N
66	A negative post is discovered on a Social Media site that has been posted by a non-employee.	Potential	Gather appropriate documentation (print-screens, dates, name of social media site, name of poster, how post was discovered). Notify Human Resources.	Notify Marketing (or customer service or public relations or branch manager) via e-mail.	Marketing will determine whether customer should be contacted.	NA	N	N	N
67	Default Action: Unforeseen Negative Incident	Potential	Notify ISO	File PIR with ISO	Investigate Source, Follow-up Report in next CIRT meeting	varies	Y	N	N
68	Other Instructions:	Potential							


Decision Tree
Reading Time!
Non-Technical Incidents (Sample)
infotex


Decision Tree
• Show 'em the excel spreadsheet!
D!
infotex

Digital Forensics

- If there is a potential for litigation:
  - Enlist a third party if possible.
  - Enlist a qualified third party if possible.
  - Chain of custody is essential.
  - Since still no good certification for digital forensics, the best way to see if a party is qualified: ask them to show you their write blocker!

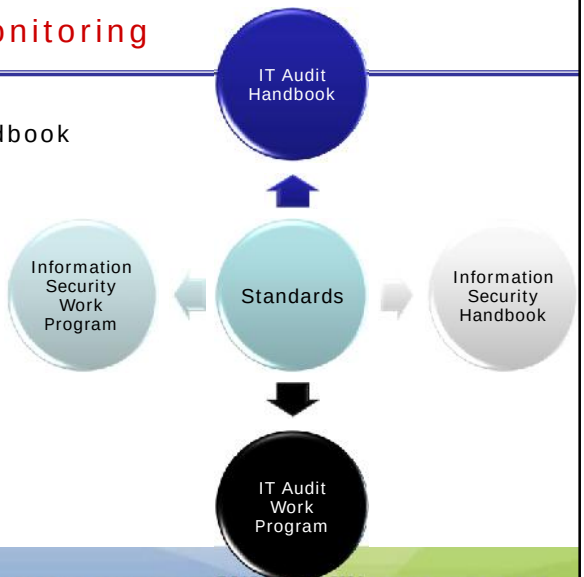
infotex

Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Framework
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

FFIEC Guidelines
for Security Monitoring

Information Security Handbook
Circa 2006



FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

Financial institutions should:

- Identify the system components that warrant logging;
- Determine the level of data logged for each component; and,
- Establish policies for securely handling and analyzing log files.

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

Financial institutions should:

- Identify the system components that warrant logging;
- Determine the level of data logged for each component; and,
- Establish policies for securely handling and analyzing log files.

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

Data to log:

- Inbound and outbound Internet traffic,
- Internal network traffic,
- Intrusion detection system events,

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

Data to log:

- Inbound and outbound Internet traffic,
- Internal network traffic,
- Intrusion detection system events,

IDS/IPS Systems

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

Data to log:

- Network and host performance,
- Operating system access (especially high-level administrative or root access),
- Application access (especially users and objects with write-and-execute privileges), and
- Remote access.

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

Data to log:

- Network and host performance,
- Operating system access (especially high-level administrative or root access),
- Application access (especially users and objects with write-and-execute privileges), and
- Remote access.

Event Logs

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

FFIEC Guidelines

- "Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by:

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

FFIEC Guidelines

- "Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by:

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

FFIEC Guidelines

- Monitoring network and host activity to identify policy violations and anomalous behavior;

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

FFIEC Guidelines

- Monitoring host and network condition to identify unauthorized configuration and other conditions which increase the risk of intrusion or other security events;

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

FFIEC Guidelines

- Analyzing the results of monitoring to accurately and quickly identify, classify, escalate, report, and guide responses to security events; and

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

FFIEC Guidelines

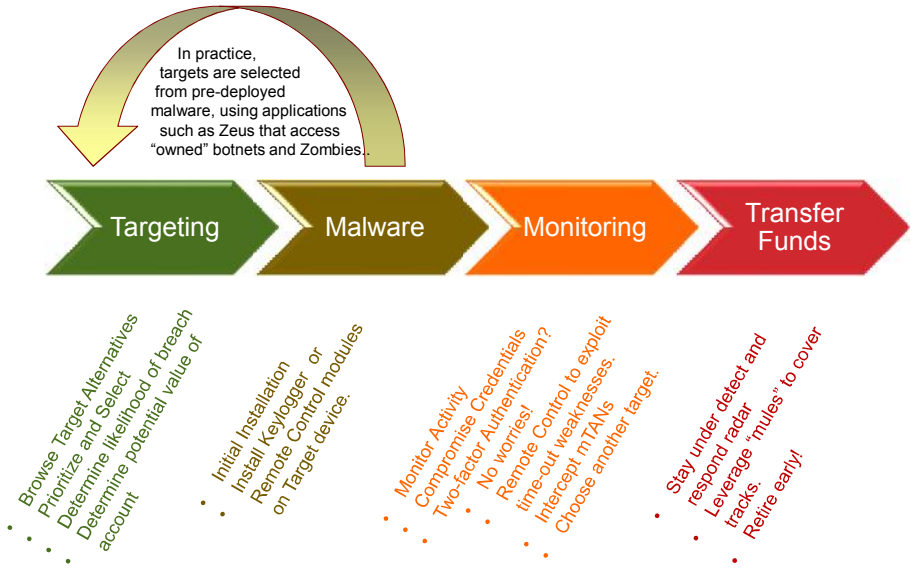
- Responding to intrusions and other security events and weaknesses to appropriately mitigate the risk to the institution and its customers, and to restore the institution's systems.

FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Framework
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

ANATOMY OF AN ATTACK (CATO)



Intrusion Timeline

How an Intrusion Happens...

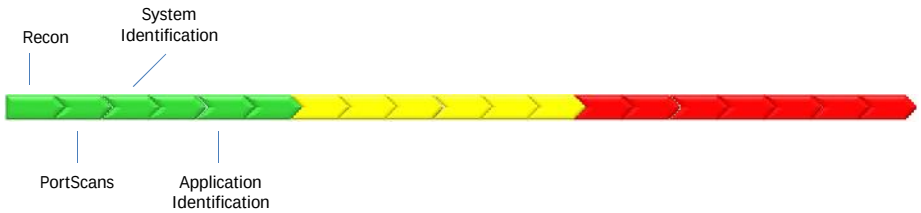
Time →

infotex

Intrusion Timeline

How an Intrusion Happens...

Time →

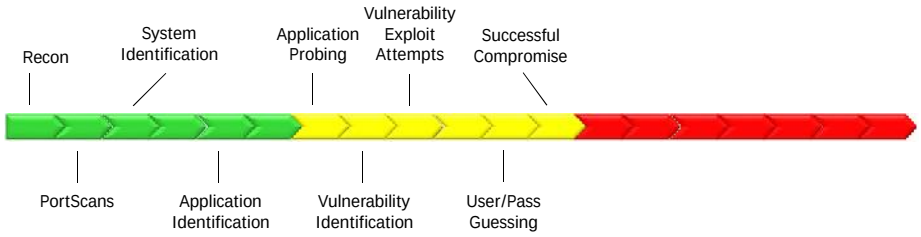


infotex

Intrusion Timeline

How an Intrusion Happens...

Time →

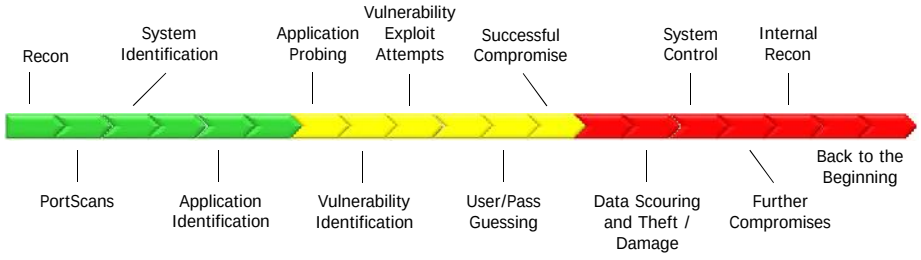


infotex

Intrusion Timeline

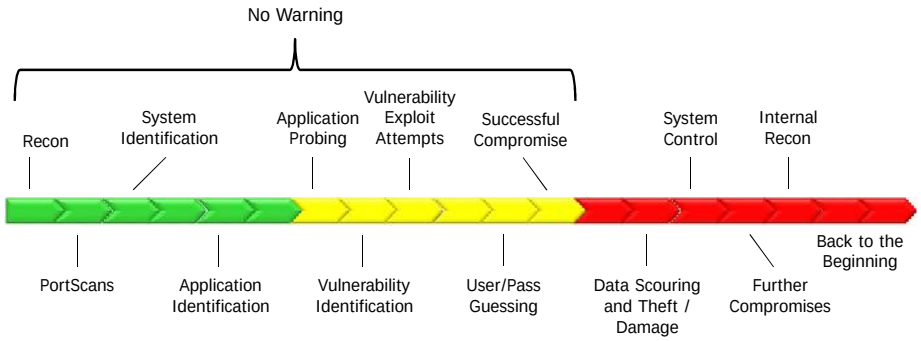
How an Intrusion Happens...

Time →



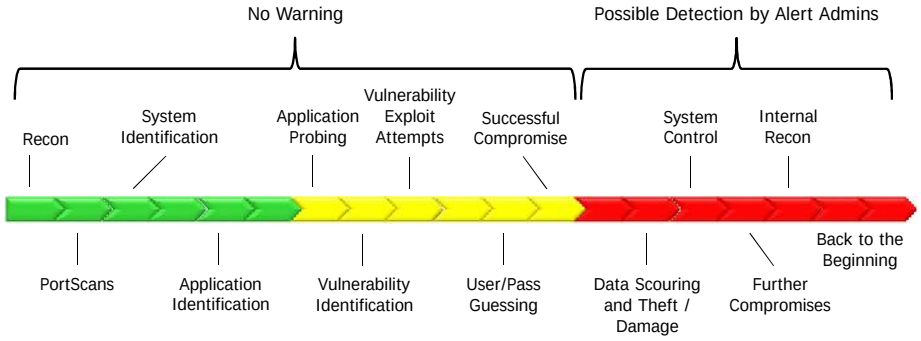
infotex

Intrusion Timeline – No Monitoring

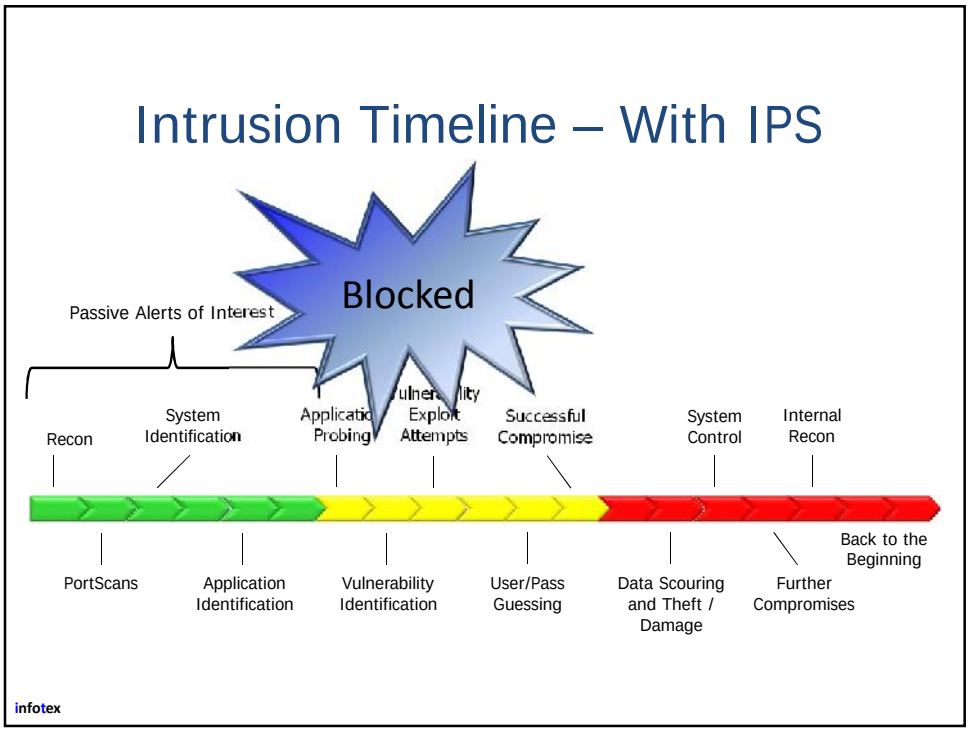


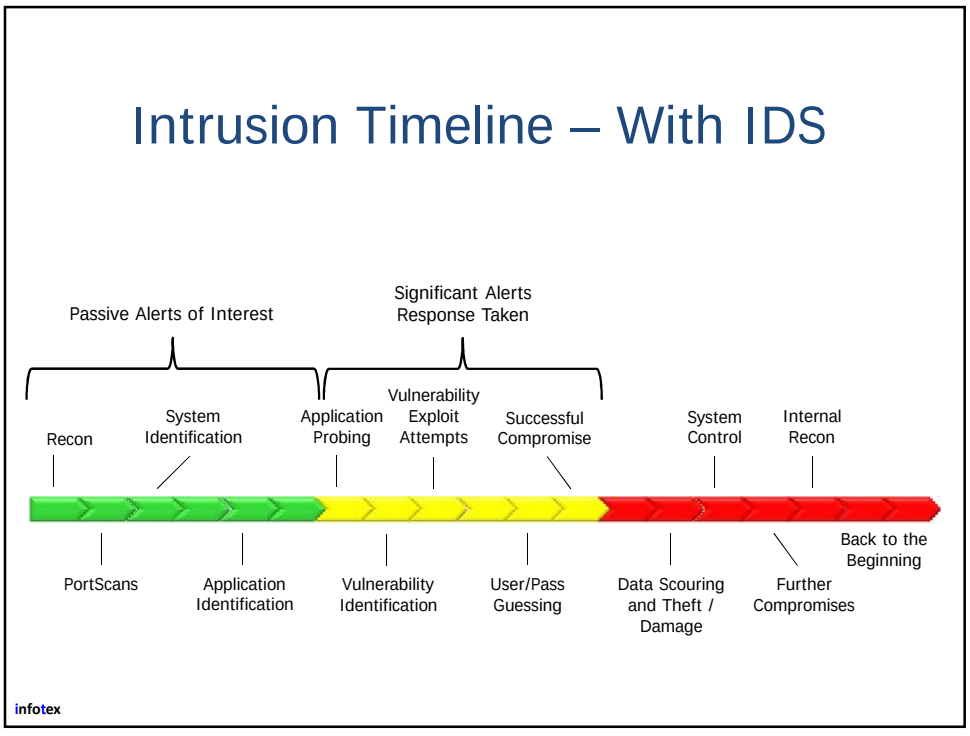
infotex

Intrusion Timeline – No Monitoring

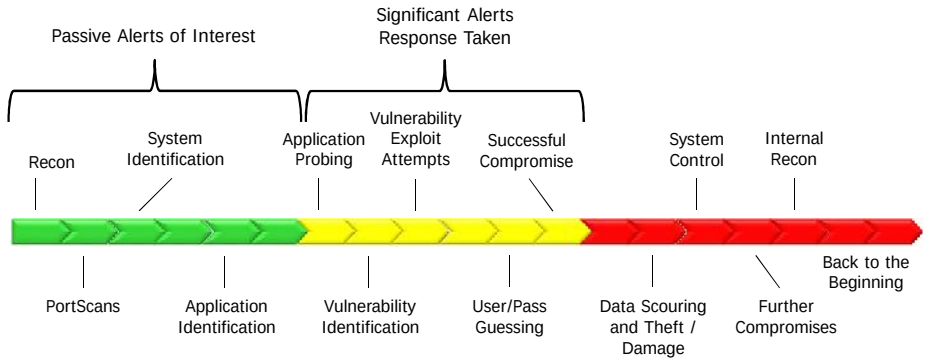


infotex


Intrusion Timeline – With IPS
Blocked
Passive Alerts of Interest
Recon
System Identification
Application Probing
Vulnerability Exploit Attempts
Successful Compromise
System Control
Internal Recon
PortScans
Application Identification
Vulnerability Identification
User/Pass Guessing
Data Scouring and Theft / Damage
Further Compromises
Back to the Beginning
infotex

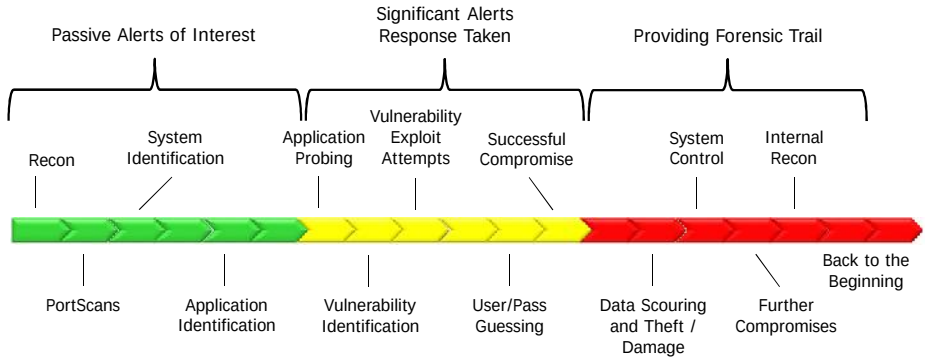

Intrusion Timeline – With IDS
Passive Alerts of Interest
Significant Alerts Response Taken
Recon
System Identification
Application Probing
Vulnerability Exploit Attempts
Successful Compromise
System Control
Internal Recon
PortScans
Application Identification
Vulnerability Identification
User/Pass Guessing
Data Scouring and Theft / Damage
Further Compromises
Back to the Beginning
infotex

Intrusion Timeline – With IDS



infotex

Intrusion Timeline – With ELM



infotex

Intrusion Prevention Considerations

- Base Architecture
  - Snort, Surricata, Proprietary
- Signature Updating
  - Zero Day Vulnerability Protection
  - Emerging Threats Signatures
  - ET Pro Commercial Signature Sets

infotex

Intrusion Detection Considerations

- Monitoring must be active 24x7x365
- Real Time Response
- Should be able to write signatures customized to your unique situation
- In the very near future, will be able to inspect SSL Traffic (in innovation phase of development right now.)

infotex

Event Log Management

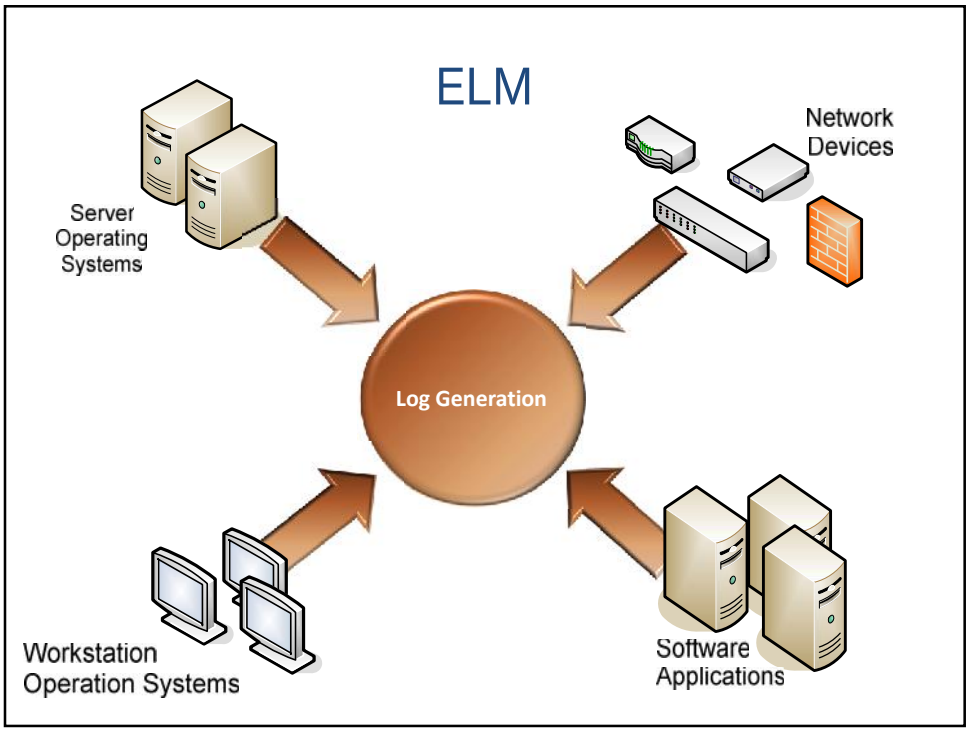
- Considerations
  - Real-time Reporting / Response
  - Forensic Archiving
  - Correlation with IDS
  - Trend Reporting Interface

infotex

Event Log Management

- Architecture
  - Logs stay on Client Network
  - Agent installed on Critical Devices
  - Archive of original, unparsed un-aggregated logs.
  - Hash on each archive file (for forensics purposes)

infotex



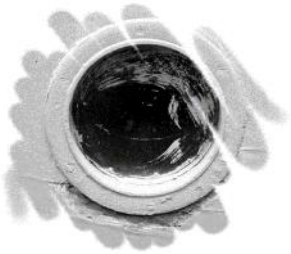
Change Detection

- Monthly or weekly scans of external IPs.
- Report will show change in ports (open or closed).
- Does not include UDP ports
- Client must confirm report.

infotex

Change Detection

- Firewall Changes
- Firewall Rules Changes
- Web Defacement Monitoring
- Specific files that should not change

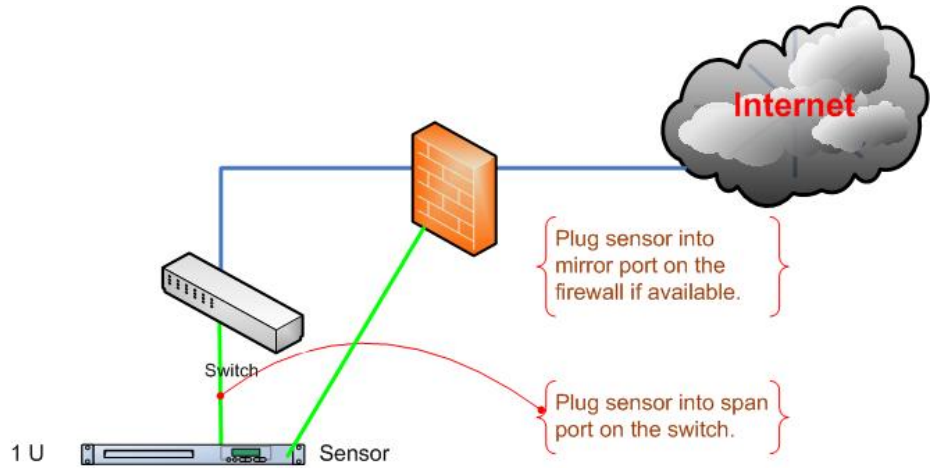


infotex

Standard IDS Configuration

No Single Point of Failure, But No Automated Blocking

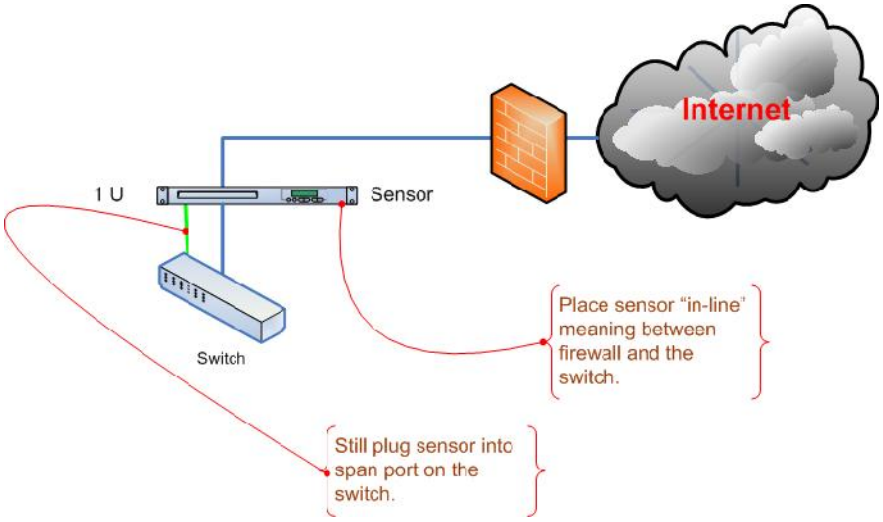
Detective Only



In-Line (IPS) Configuration

Introduces Single Point of Failure

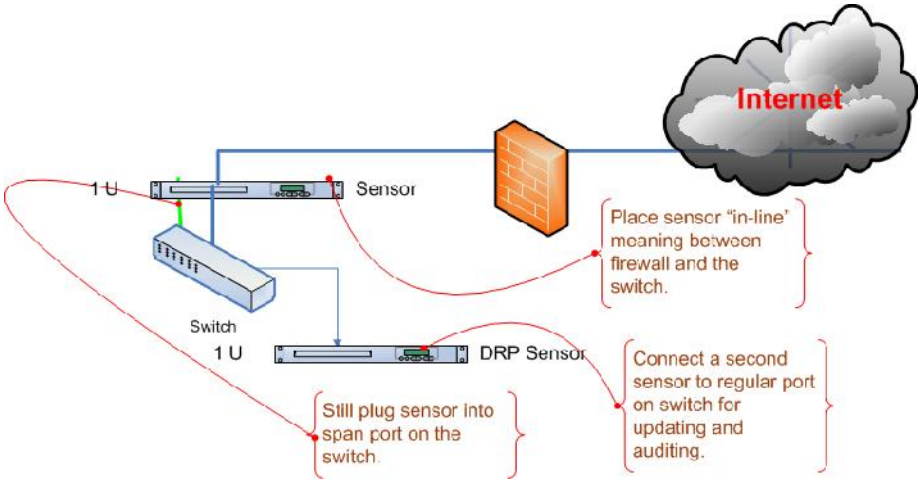
Preventive and Detective



Redundant In-Line (IPS) Configuration

Still a Single Point of Failure, But with Redundant Updated Sensor

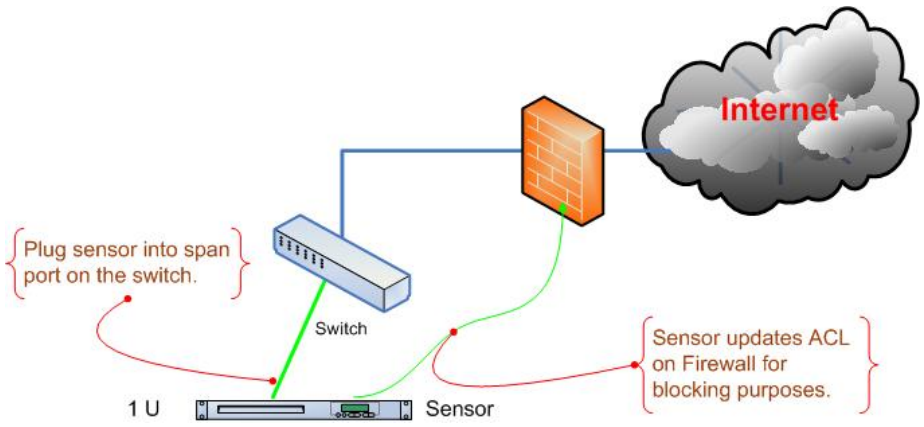
Preventive and Detective



Dynamic ACL Updating

No Single Point of Failure, With Automated Blocking

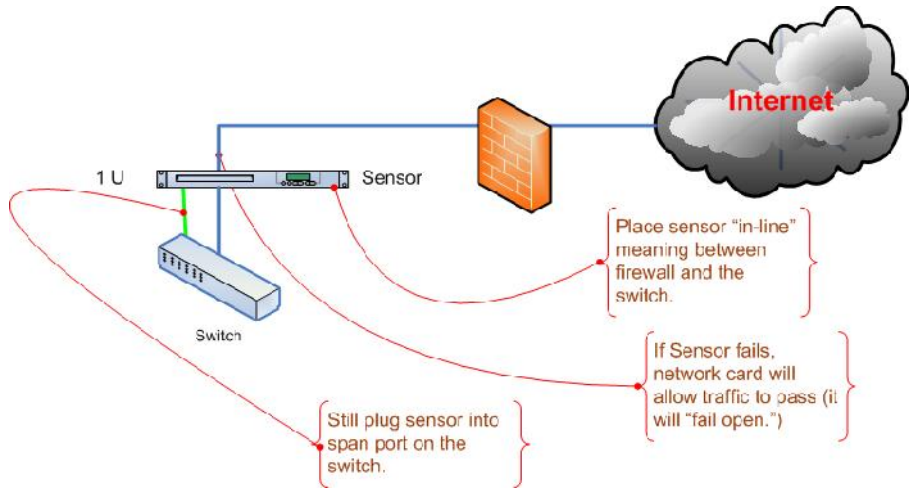
Preventive and Detective



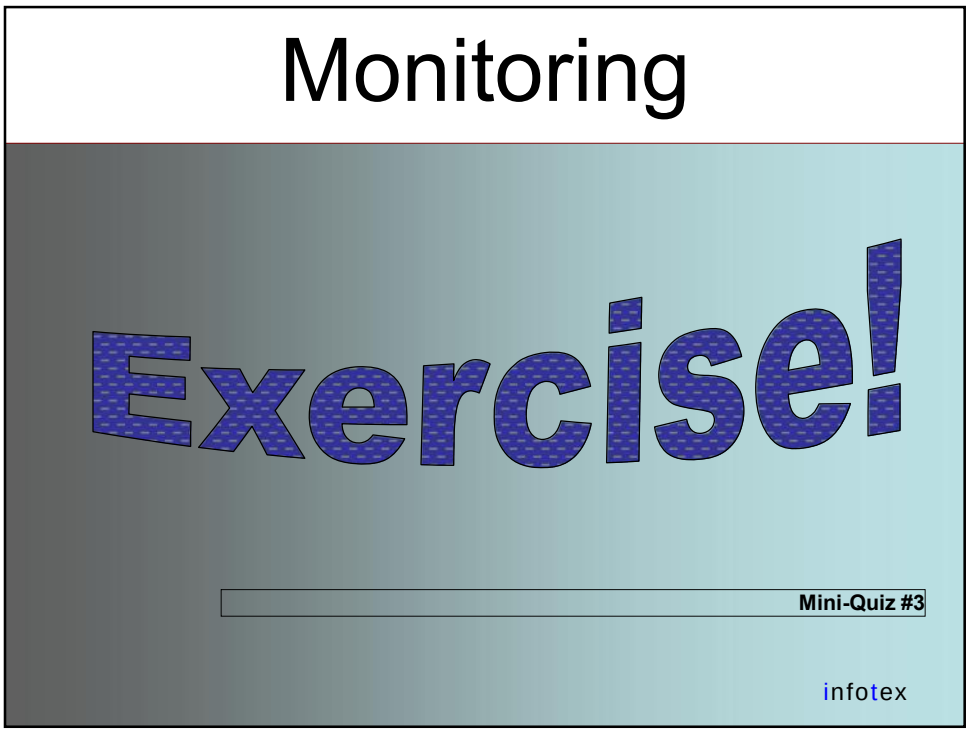
LAN Bypass Configuration

No Single Point of Failure, Protection Bypassed

Preventive and Detective



Quick!
Reading Time!
Managed Security Service Providers
infotex


Monitoring
Exercise!
Mini-Quiz #3
infotex

Here is a list of Intrusion Detection / Intrusion Prevention service providers. Note that this list is NOT all-inclusive.

DataComm
Website: www.datacomm.com
Address:
6801 N. 54th St.
Tampa, FL 33610
Phone: (800) 544-4627

Fortinet
Website: www.fortinet.com
Address:
1090 Kifer Rd.
Sunnyvale, CA 94086
Phone: (866) 868-3678

infotex
Website: www.infotex.com
Contact: Dan Hadaway
E-mail address: dhadaway@infotex.com
Address:
2366 W. Boulevard
Kokomo, IN 46902-2147
Phone: (800) 466-9939

Perimeter
Website: www.perimeterusa.com
Address:
440 Wheelers Farms Road, Suite 202
Milford, CT 06460
Phone: (800) 234-2175

Secure Works, Inc. (Dell)
Website: www.secureworks.com
Sales Contact: Scott Ernst
E-mail Address: sernst@secureworks.com
Address:
11 Executive Park
Atlanta, GA 30329
Phone: (404) 486-4453

Trustwave
Website: www.trustwave.com
Address:
70 West Madison St., Suite 1050
Chicago, IL 60602
Phone: (312) 873-7500

Here is a sample list of Event Log Management service providers. Note that this list is NOT all-inclusive.

infotex
Website: www.infotex.com
Contact: Dan Hadaway
E-mail address: dhadaway@infotex.com
Address:
2366 W. Boulevard
Kokomo, IN 46902-2147
Phone: (800) 466-9939

EventSentry
Netikus.net Ltd. (Corporate)
Website: www.eventsentry.com
Address:
225 W. Washington St., Suite 2200
Chicago, IL 60606
Phone: (877) NETIKUS

GFI
Website: www.gfi.com
Address:
15300 Weston Parkway, Suite 104
Cary, NC 27513
Phone: (888) 243-4329

LogLogic
Website: www.loglogic.com
Address:
110 Rose Orchard Way, Suite 200
San Jose, CA 95134
Phone: (888) 347-3883

Secure Works, Inc. (Dell)
Website: www.secureworks.com
Sales Contact: Scott Ernst
E-mail Address: sernst@secureworks.com
Address:
11 Executive Park
Atlanta, GA 30329
Phone: (404) 486-4453

Risk Monitoring Architecture:
Place an X by those monitoring controls that you have in place:

_____ Patch Management is monitored by external audit testing.

_____ Patch Management is monitored by internal audit testing on a _____ basis.
(quarterly, monthly)

_____ At least one layer of Anti-Virus, Anti-Spam, or UTM (Unified Threat Management).

_____ Intrusion Prevention System on the Firewall

_____ Intrusion Prevention Segregated from the Firewall

_____ Intrusion Detection on the Perimeter

_____ Intrusion Detection on the Internal Network

_____ Host-based Intrusion Detection or Intrusion Prevention (an IPS and/or IDS sensor in front of a particular host, guarding only that host.)

_____ Application-based Firewalls on Endpoints (ie: Windows Firewall Enabled)

_____ SIEM or Event Log Management (consolidating and analyzing logs for critical assets.)

_____ Manual Log Monitoring

_____ Change detection on the Firewall

_____ Change detection on the firewall rules

_____ Web Defacement Monitoring

_____ Other File Integrity Checking Systems (inventory here: _____

_____

_____ Network Flow Analysis

_____ Third party monitoring solutions in place (inventory here: _____

_____

- _____ At least one person on the IRT is assigned to monitor FS-ISAC.
- _____ At least one person on the IRT is assigned to monitor for policy violations.
- _____ At least one person on the IRT is assigned to monitor for awareness issues.
- _____ At least one person on the IRT belongs to an organization like CERT, Infragard, etc.

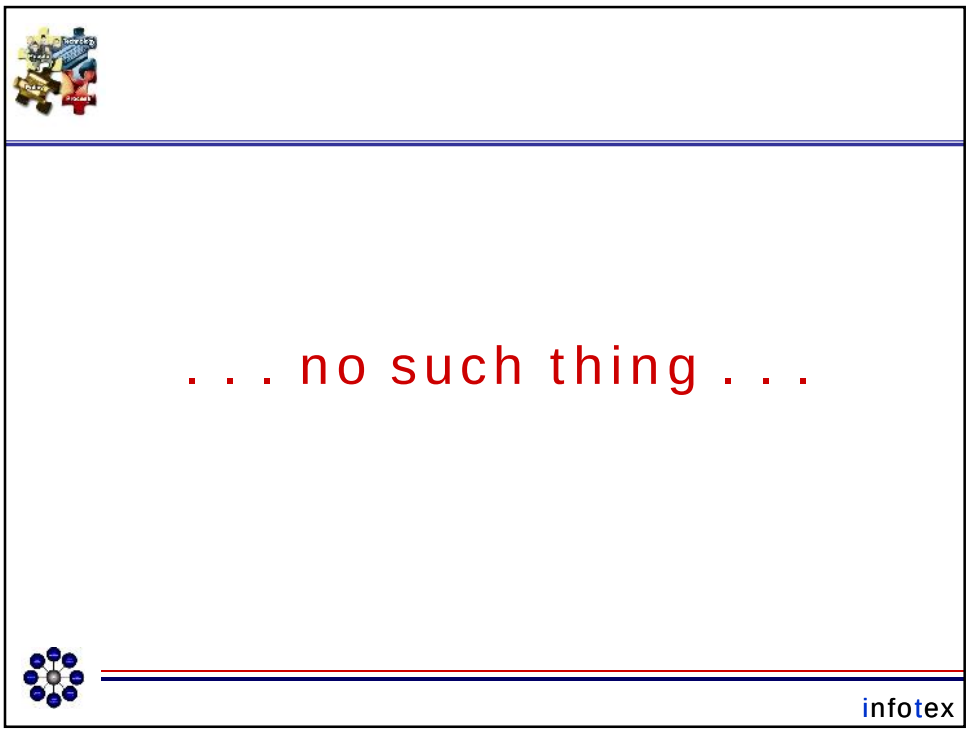
_____ A forensics company has been retained to assist in the collection and preservation of evidence.

_____ Our attorney attends our Incident Respone Teams on a regular basis.

_____ Our MSSP attends our Incident Respone Teams on a regular basis.

Do we need a break?

Today's Agenda
• The Workshop and the Workbook
• Incident Response Fundamentals
– Future Compliance Frameworks
• Incident Response Program
– Policy Considerations
– Response Procedures
– Customer Notification
• Risk Monitoring
– The FFIEC Risk Monitoring Requirements
– Anatomy of an Attack
– Non-technical Risk Monitoring
– The NIST Frameworks
– Documenting a Risk Monitoring Architecture
• Putting it all to work!


. . . no such thing . . .
infotex

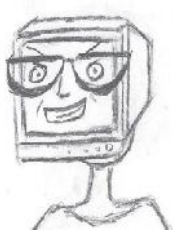
Non-Technical Incidents

- Malicious, Non-malicious, Accidental
- Policy Violation
- Suspicious Activity
- Potential Incidents
- Technology Incidents

infotex

Non-Technical Incidents

- Malicious
  - Physical Breach Attempt
  - Pretext Calling
  - Phishing Attempt
    - On the bank
    - On the bank's customers
  - Malware (not discovered by technical security controls)



infotex

Non-Technical Incidents

- Policy Violations
  - Unlocked workstations found.
  - Written passwords found.
  - Forwarded jokes, e-chain letters, etc.
  - Employee observed with a prohibited device (such as a USB drive or iPod connected to workstation).

infotex

Non-Technical Incidents

- Policy Violations
  - Offensive/illegal files found.
  - Unlicensed software found.
  - Company software installed at home.
  - Other improper personal use of company resources.

infotex

Non-technical Incidents

- Suspicious Activity
  - Any of the previous malicious activities.
  - Somebody taking pictures in the branch?
  - Somebody plugging a device into a network jack?

infotex

Non-technical Incidents

- Technology Incidents
  - Customer asks a question about our technology and we don't know the answer.
  - A user discovers a problem with an application that requires immediate attention.
  - A new technology, system, or device causes an unforeseen problem.

infotex

Put the IRT on notice

- Consider a high-level policy that Management "put the Incident Response Team on notice" anytime:
  - A new technology is deployed.
  - A new product or service is deployed.
  - A major system is updated.

infotex

Non-technical Incidents

- Potential Incidents
  - Stolen or lost portable device (such as laptop, Smart Phone, iPad).
  - Stolen or lost backup tape, or any other medium with sensitive information.
  - A customer accuses us of leaking sensitive information, even if/when we did not leak the information.

infotex

Non-technical Incidents

- Potential Incidents
  - A negative post is discovered on a Social Media site that has been posted by an employee.
  - A negative post is discovered on a Social Media site that has been posted by a non-employee.

infotex

Let's go around the room

- What other non-technical incidents can you think of?

infotex

Do we need a break?

infotex

Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Frameworks
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

NIST Frameworks

- NIST SP 800-61 (Incident Response)
- The NIST CyberSecurity Framework

NIST Frameworks

- NIST SP 800-61 (Incident Response)
- The NIST CyberSecurity Framework

NIST SP 800-61

- Precursors and Indicators
  - Search for “3.2.3”

Let’s see the regs!

NIST Sources of Pre-cursors and Indicators

- IDPSs (alerts)
- SIEMs (logs)
- AVS/Anti-Spam
- File Integrity Checking Software
- Third Party Monitoring Services
- Threat Intelligence
- People

NIST SP 800-61

infotex

IDPS (IPS/IDS)

- Identify suspicious events and record pertinent data regarding them, including
  - the date and time the attack was detected,
  - the type of attack,
  - the source and destination IP addresses, and the username (if applicable and known).

NIST SP 800-61

infotex

IDPS (IPS/IDS)

- Signature Based
  - Signature database must be maintained,
  - Attacks must be known (recognizable)
- 99.999% False Positives
- Requires Gray Matter

31

NIST SP 800-61

infotex

REQUIRES Gray Matter

Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.

NIST SP 800-61

infotex

Technology Staff

Often Understaffed

- No Time
- Everything Urgent

Focused Elsewhere

- Reliability, Upgrades, Convenience
- New Products, Services

Lacking Security Skills

- Inability to stay current
- Focused Elsewhere

MSSP: Sleep at Night!

- Continuous Monitoring, Instant Response
- No turnover, vacations, benefits
- Dedicated, trained, certified professionals who do nothing but watch networks
- 24 x 7 (not daily, weekly, or monthly)

- Focus: As threats change, we change

infotex

Segregation of Duties

- Network Administration should manage the firewall.
- Somebody Else should watch the firewall.

- Same with server configurations, network device configurations, etc.
- Same with forensic evidence collection and preservation.

infotex

Defining SIEM

- First, pronouncing SIEM
- Each vendor defines it differently.
- We see it as a buzzword for Incident Response Management overall.

- What we want: cross-checking threat intelligence with real-time data from your network as well as non-technical event data.

infotex

How NIST defines a SIEM

- Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data (see logs below).

NIST SP 800-61

infotex

File Integrity Checking Software

- Change Detection directed at specific files (or groups of files)
- Web Defacement Monitoring
- Monitoring for changes in firewall ruleset.
- Monitoring for changes in important files that must remain static.

NIST SP 800-61

infotex

Third Party Monitoring

- Actually, NOT your MSSP
- Companies and organizations that monitor for specific types of fraud, crime, or incidents
- Many are free or association-based
- Many more are commercial

NIST SP 800-61

infotex

NIST on LOGS

- Operation System, Service, and Application Logs
- Network Device Logs
- Network Flows

NIST SP 800-61

infotex

Network Flow

- Communication sessions occurring between hosts.
- Anomalous network flow can be caused by malware, data exfiltration, and other malicious acts.
- There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.

NIST SP 800-61

infotex

Vulnerability News

- NIST calls this “Information on new vulnerabilities and exploits.”
  - National Vulnerability Database (NVD)
  - US-CERT

(There are many others, we’ll go over a few later in the workshop.)

NIST SP 800-61

infotex

People

- From within the organization
  - Users, System Administrators
  - Incident Response Team (IRT)
  - Facilitate Internal Reporting
  - Validate every suspicion

infotex

People

- From outside the organization
  - Customers, External Users
  - Other organizations'' IRT's
  - Facilitate external reporting
  - Validate every suspicion

infotex

Is NIST 800-61 the end then?

- No.
- A special publication is not a framework.
- And the NIST 800-61 would lead to a weak posture, because it is not “integrated” with the rest of the IT Governance Processes.

infotex

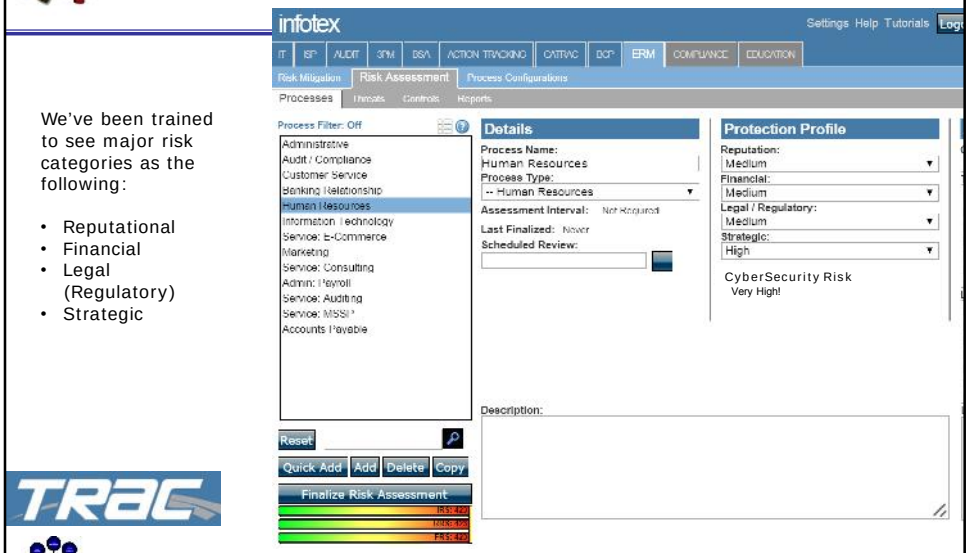
NIST Frameworks

- NIST SP 800-61 (Incident Response)
- The NIST CyberSecurity Framework

Wants to be a Category

We've been trained to see major risk categories as the following:

- Reputational
- Financial
- Legal (Regulatory)
- Strategic

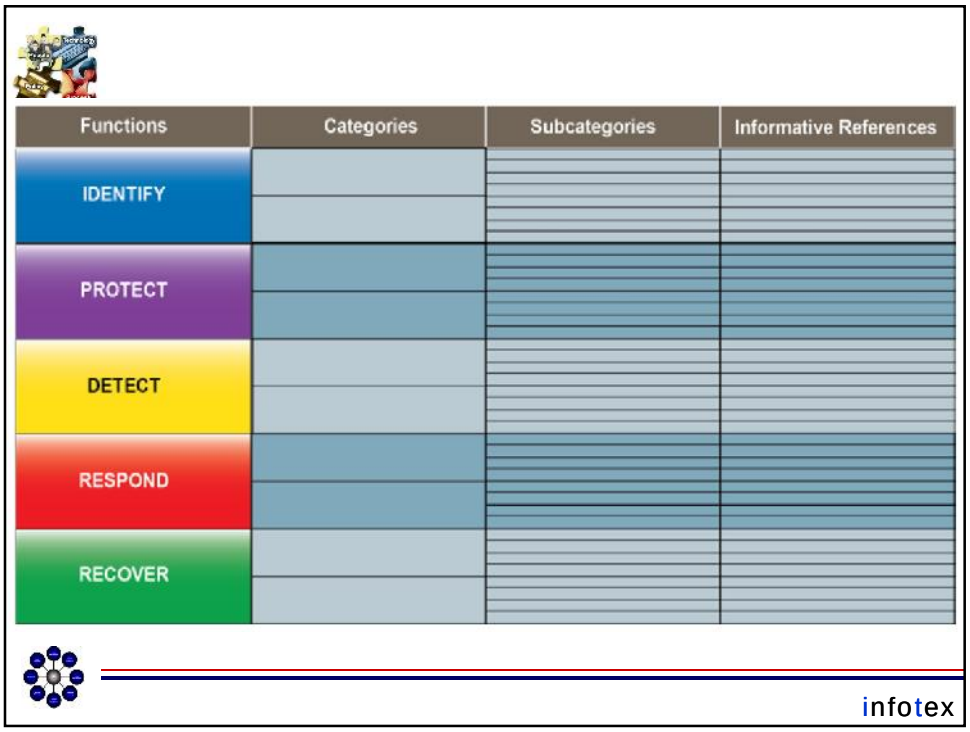


TRAC

infotex

The Framework

Let's see the regs!



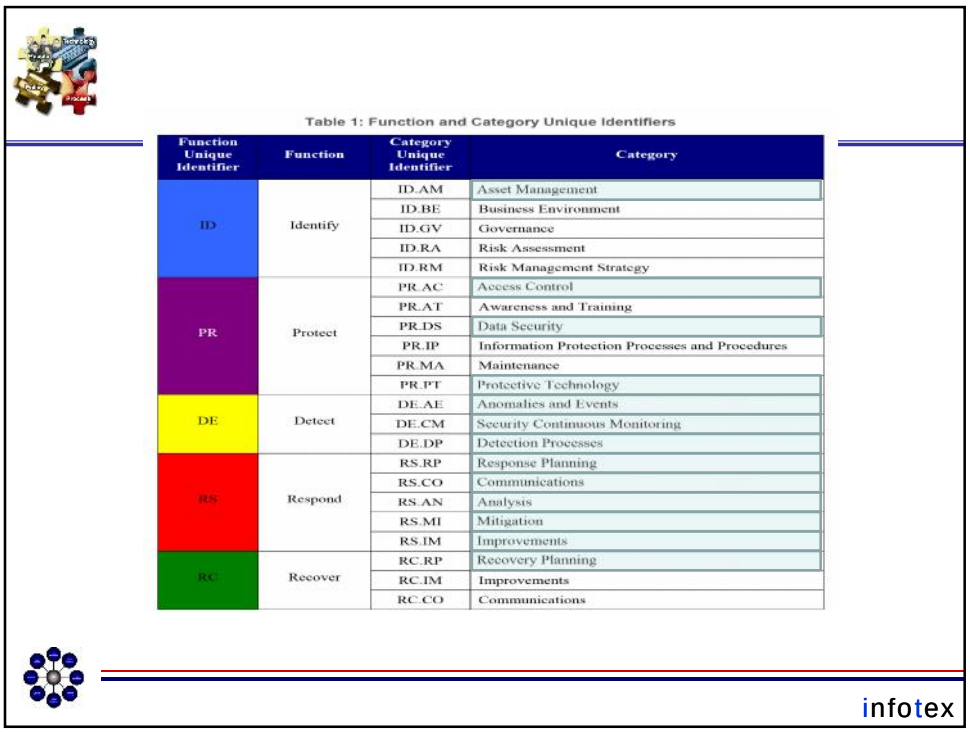


Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Simplify IT

- Five Functions of CyberSecurity Controls
  1. Identify
  2. Protect
  3. Detect
  4. Respond
  5. Recover

infotex

What we mean by "covered"

- If the text is highlighted by a "pink rectangle" then this particular NIST CyberSecurity Framework Subcategory is "supported" by our process. We either have the ability to help you, but you need to ask for our help, or our processes deliver information that can help you with the process.

- If the text is highlighted in blue, then our contractual arrangement with you (assuming you have full coverage*) requires us to implement all or part of this NIST CyberSecurity Framework Subcategory.

infotex

Full Coverage

- Intrusion Prevention on the Perimeter
  - (Our sensor in blocking mode in front of your firewall)
- Intrusion Detection on the Perimeter
- Intrusion Detection on Internal Traffic
- Event Log Management of all Critically Classified Devices
- Change Detection
- Policy Development Kit
- Incident Response Team Maintenance Contract
- Web Defacement Monitoring
- Forensics Retainer

infotex

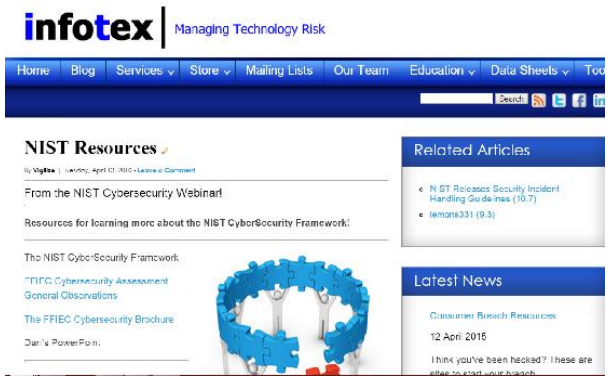
Full Coverage

- Intrusion Prevention on the Perimeter
  - (Our sensor in blocking mode in front of your firewall)
- Intrusion Detection on the Perimeter
- Intrusion Detection on Internal Traffic
- Event Log Management of all Critically Classified Devices
- Change Detection
- Policy Development Kit
- Incident Response Team Maintenance Contract
- Web Defacement Monitoring
- Forensics Retainer

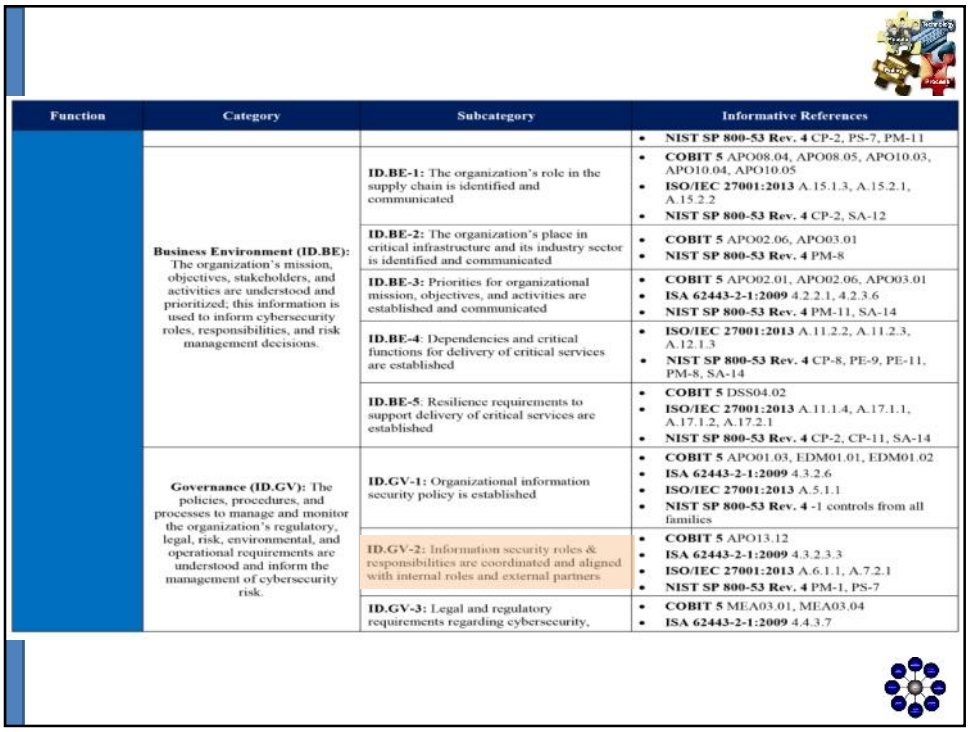
infotex

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev.** [illegible]2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

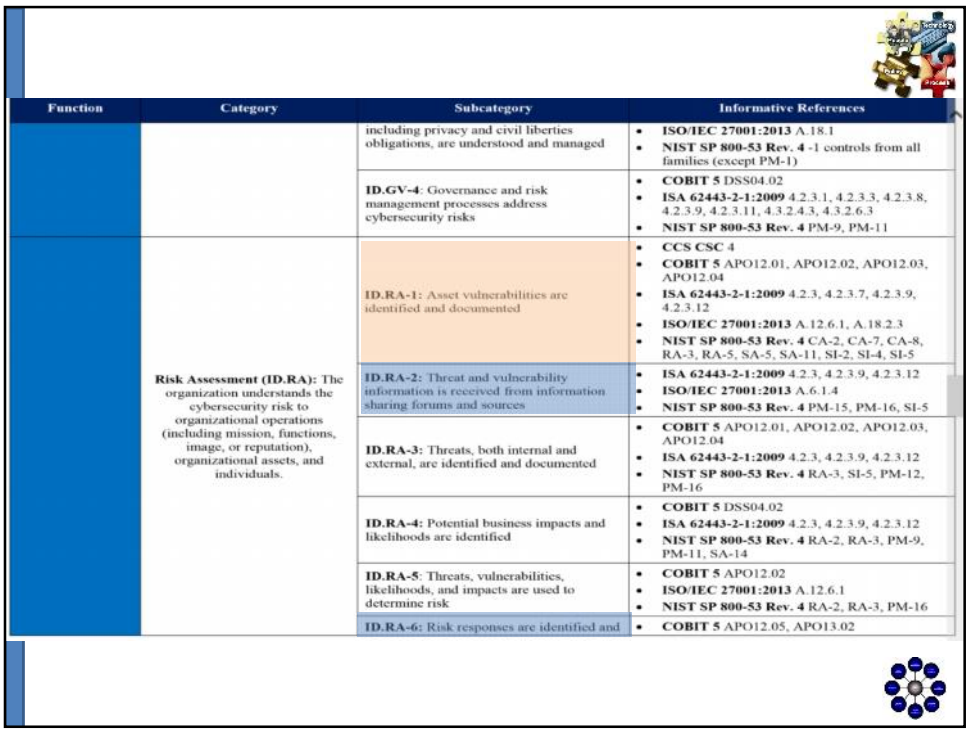
Resources – my.infotex.com/nist-resources



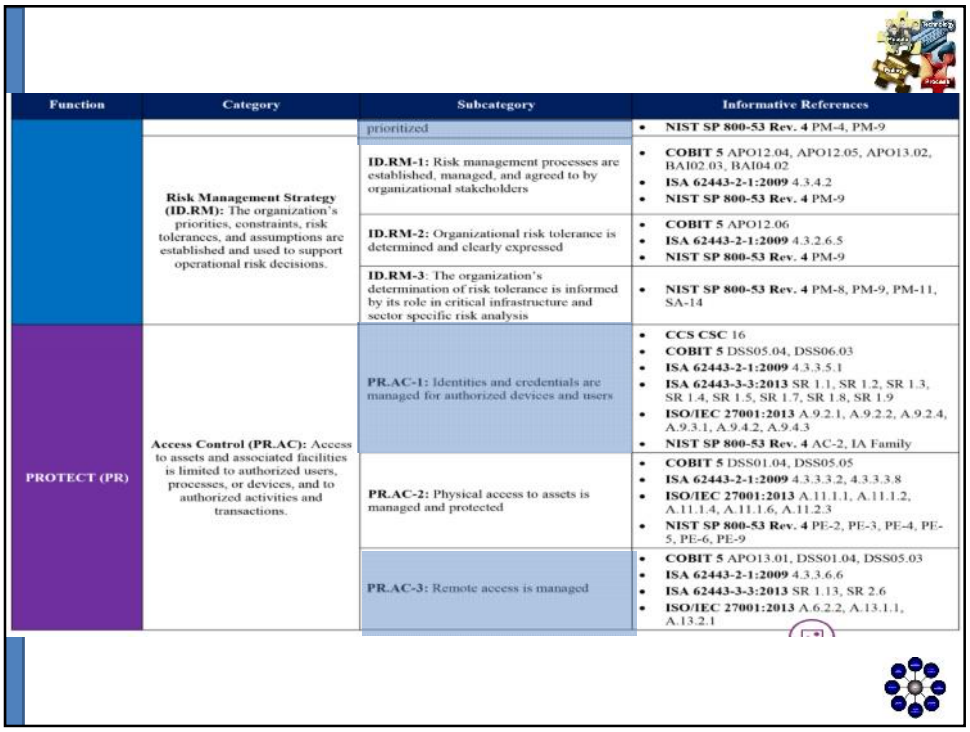
infotex



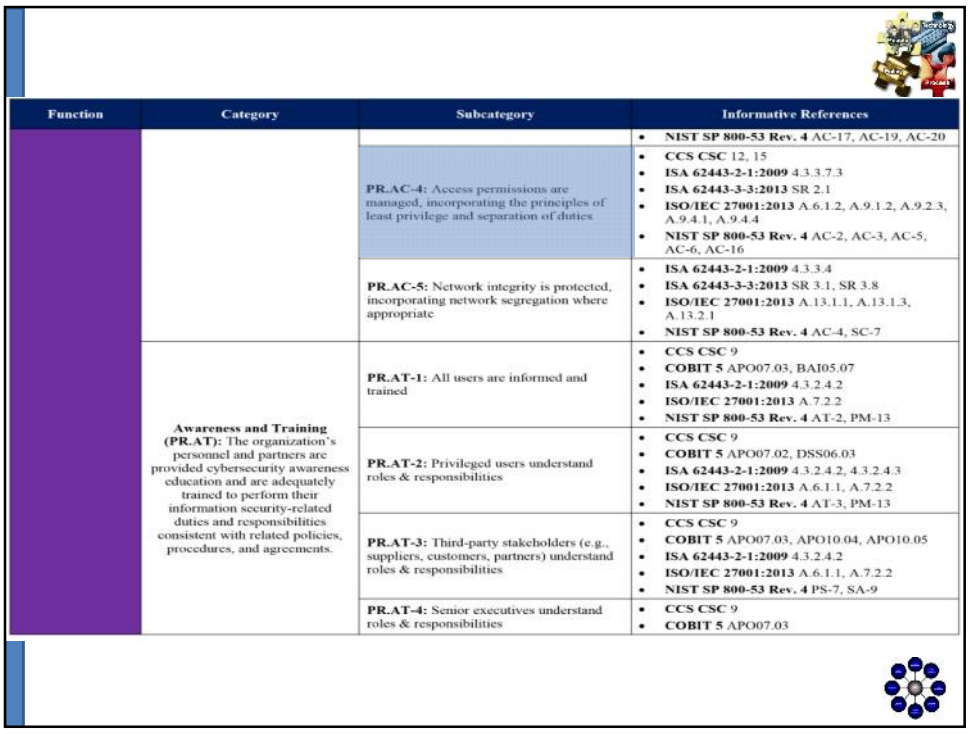
Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	• **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• **COBIT 5** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• **COBIT 5** APO02.01, APO02.06, APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 • **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	• **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 • **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	• **COBIT 5** DSS04.02 • **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	• **COBIT 5** APO01.03, EDM01.01, EDM01.02 • **ISA 62443-2-1:2009** 4.3.2.6 • **ISO/IEC 27001:2013** A.5.1.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• **COBIT 5** APO13.12 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity,	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7



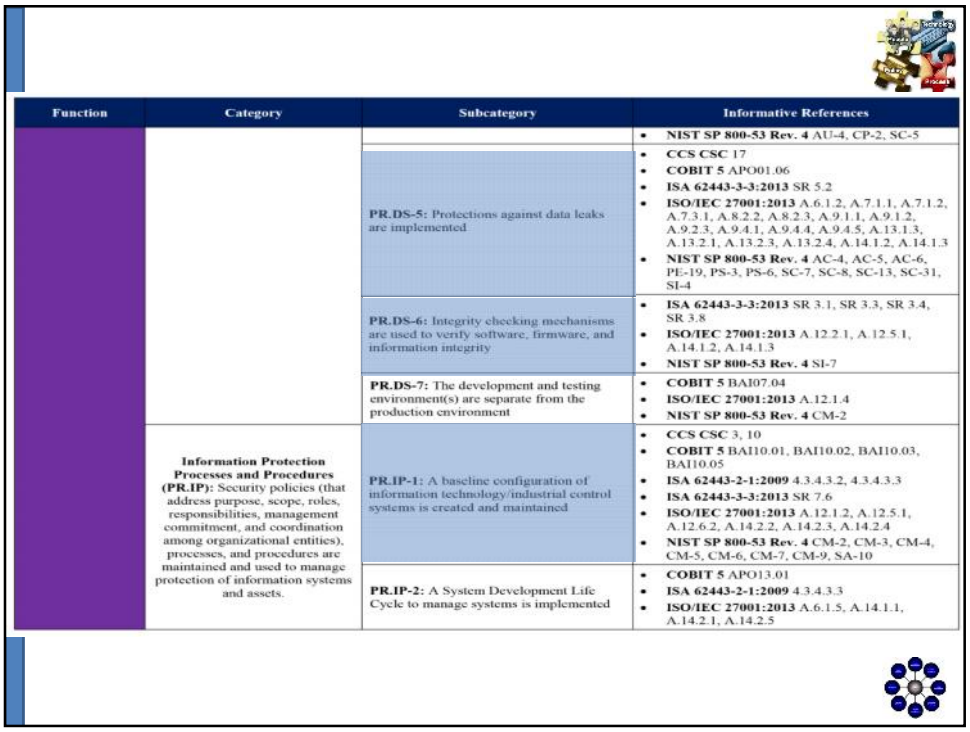
Function	Category	Subcategory	Informative References
		including privacy and civil liberties obligations, are understood and managed	• **ISO/IEC 27001:2013** A.18.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • **NIST SP 800-53 Rev. 4** PM-9, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	• **CCS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	• **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	• **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and	• **COBIT 5** APO12.05, APO13.02



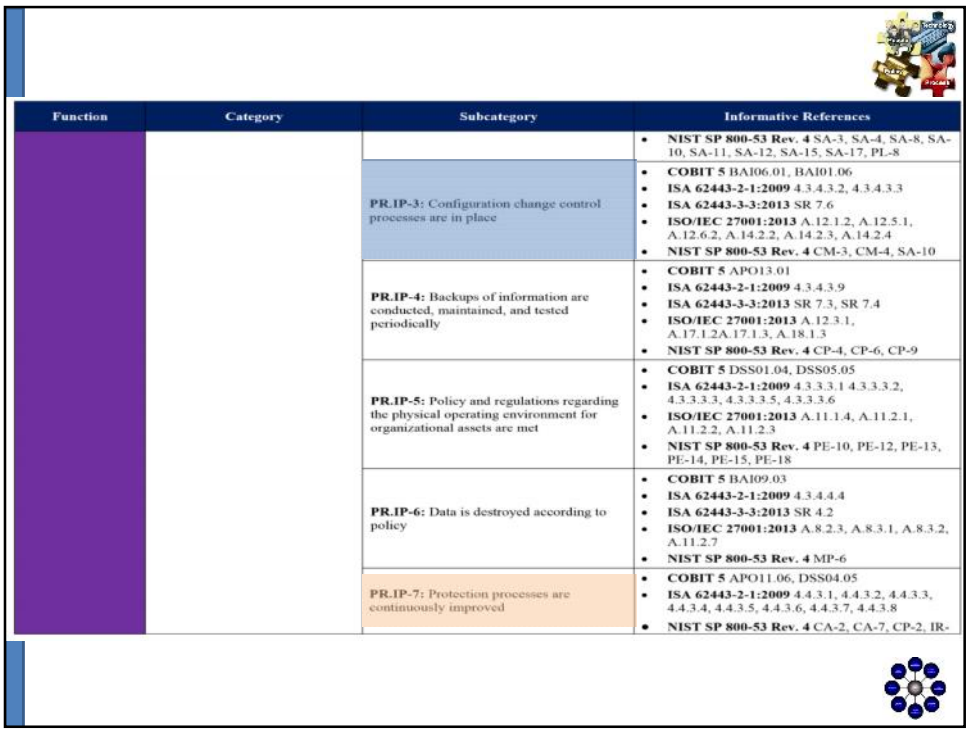
Function	Category	Subcategory	Informative References
		prioritized	• **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	• **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.2.6.5 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1



Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	• **CCS CSC** 12, 15 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	• **ISA 62443-2-1:2009** 4.3.3.4 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, SC-7
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	• **CCS CSC** 9 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03



Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	• **CCS CSC** 17 • **COBIT 5** APO01.06 • **ISA 62443-3-3:2013** SR 5.2 • **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 • **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	• **COBIT 5** BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	• **CCS CSC** 3, 10 • **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.3 • **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5



Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	• **COBIT 5** BAI06.01, BAI01.06 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: Protection processes are continuously improved	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-

Function	Category	Subcategory	Informative References
			8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	• **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• **COBIT 5** DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		PR.IP-10: Response and recovery plans are tested	• **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 • **NIST SP 800-53 Rev. 4** PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	• **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3.7 • **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1

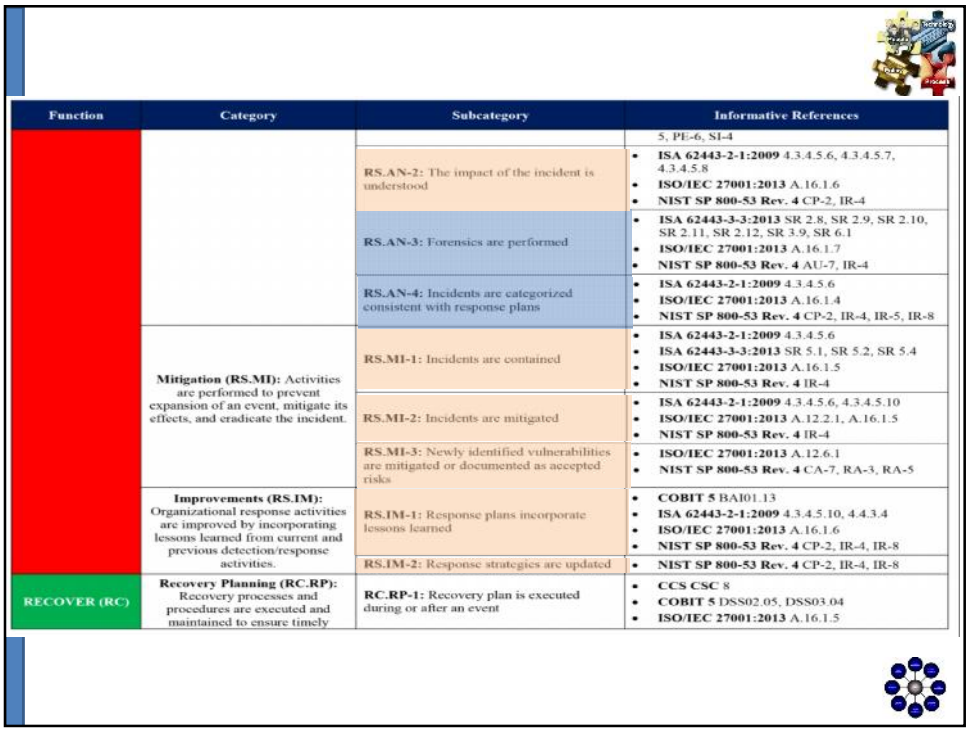
Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• **CCS CSC** 14 • **COBIT 5** APO11.04 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	• **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 2.3 • **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	• **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	• **CCS CSC** 7 • **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1,

Function	Category	Subcategory	Informative References
			SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	• **ISA 62443-3-3:2013** SR 6.1 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI - 4
		DE.AE-5: Incident alert thresholds are established	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• **CCS CSC** 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is	• **ISA 62443-2-1:2009** 4.3.3.3.8

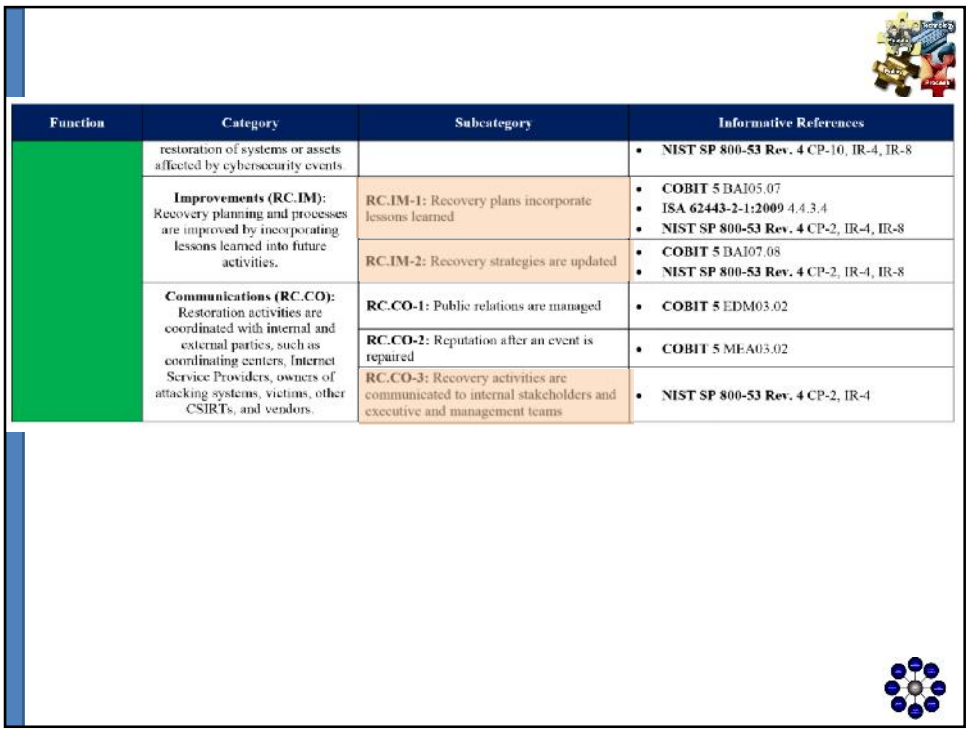
Function	Category	Subcategory	Informative References
		monitored to detect potential cybersecurity events	• **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.3.4.3.8 • **ISA 62443-3-3:2013** SR 3.2 • **ISO/IEC 27001:2013** A.12.2.1 • **NIST SP 800-53 Rev. 4** SI-3
		DE.CM-5: Unauthorized mobile code is detected	• **ISA 62443-3-3:2013** SR 2.4 • **ISO/IEC 27001:2013** A.12.5.1 • **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	• **COBIT 5** APO07.06 • **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 • **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	• **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	• **COBIT 5** BAI03.10 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1

Function	Category	Subcategory	Informative References
	adequate awareness of anomalous events.		• **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	• **ISA 62443-2-1:2009** 4.4.3.2 • **ISO/IEC 27001:2013** A.18.1.4 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Detection processes are tested	• **COBIT 5** APO13.02 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.14.2.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.9 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	• **COBIT 5** BAI01.10 • **CCS CSC** 18 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• **NIST SP 800-53 Rev. 4** PM-15, SI-5
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	• **COBIT 5** DSS02.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-



Function	Category	Subcategory	Informative References
			5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	• **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • **ISO/IEC 27001:2013** A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Incidents are mitigated	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 • **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	• **COBIT 5** BAI01.13 • **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely	**RC.RP-1:** Recovery plan is executed during or after an event	• **CCS CSC** 8 • **COBIT 5** DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5



Function	Category	Subcategory	Informative References
	restoration of systems or assets affected by cybersecurity events.		• **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	• **COBIT 5** BAI05.07 • **ISA 62443-2-1:2009** 4.4.3.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	• **COBIT 5** BAI07.08 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	• **COBIT 5** EDM03.02
		RC.CO-2: Reputation after an event is repaired	• **COBIT 5** MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	• **NIST SP 800-53 Rev. 4** CP-2, IR-4

Conclusion

- Your Managed Security Service Provider (MSSP), when used with a SIEM and full coverage, can help you comply with 69 of the “basic processes” required by the NIST CyberSecurity Framework.
- That’s 69 of 98 processes.
- (And thus, we say the Framework is “incident management heavy.”)

infotex

Primary Differences

1. Inventory of connections as well as other information assets.
2. Identification of information that should be encrypted at rest.
3. Testing of Incident Response Planning
4. More robust network monitoring beyond IPS/IDS on perimeter
   1. IDS on the internal network
   2. Event Log Management
   3. Change Detection on Firewall
5. Method of analyzing and responding to threats as they arise.
6. Awareness Training for the Board of Directors, Incident Response Team, and other “entities” besides our users and customers.

infotex

Resources – my.infotex.com/nist-resources

infotex
© 2014, 2015 Infotex Inc. All rights reserved.

Conclusion

- The Cybersecurity Assessment Tool is indeed based on the NIST Framework.
  - The language was not matched up exactly.
  - There is a map so you can see how it was derived.
- However, we do not see anything requiring that Cybersecurity be added as a new risk category in Enterprise Risk Management.

FFIEC Cybersecurity Assessment Tool

Today's Agenda

- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Frameworks
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Monitoring is Listening

- Enlist Your Team
  - Broadcast Awareness
  - Fighting the Noise
- Formal Incident Reporting
- Incident Response Team
- Information Sharing
  - FS-ISAC
  - Vulnerability News
- Training
- Auditing
- Conferences
- MSSPs (outsourced)

Non-technical Monitoring

- Policy Violation
- Awareness Issues
- Internal Risks
- Training Needs
- Global Threat/Incident Awareness (FS-ISAC, CERT, Infragard, etc.)

Let's see some of the things we do!

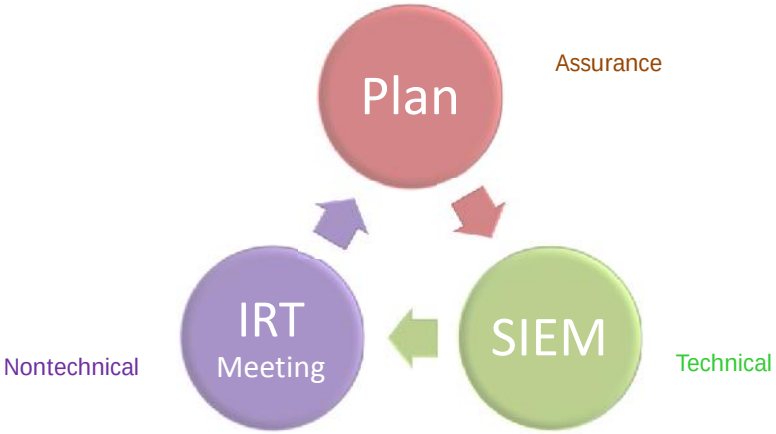
Technical Monitoring

- Vulnerabilities (and Patches)
- Network Traffic
  - Scans, Malware, Policy Violations
- Event Logs (SIEM)
  - Critical Servers, Network Devices, Workstations
  - Applications
- Security Tools
  - Firewall (changes, events, vulnerabilities, etc.)
  - AVS, UTM

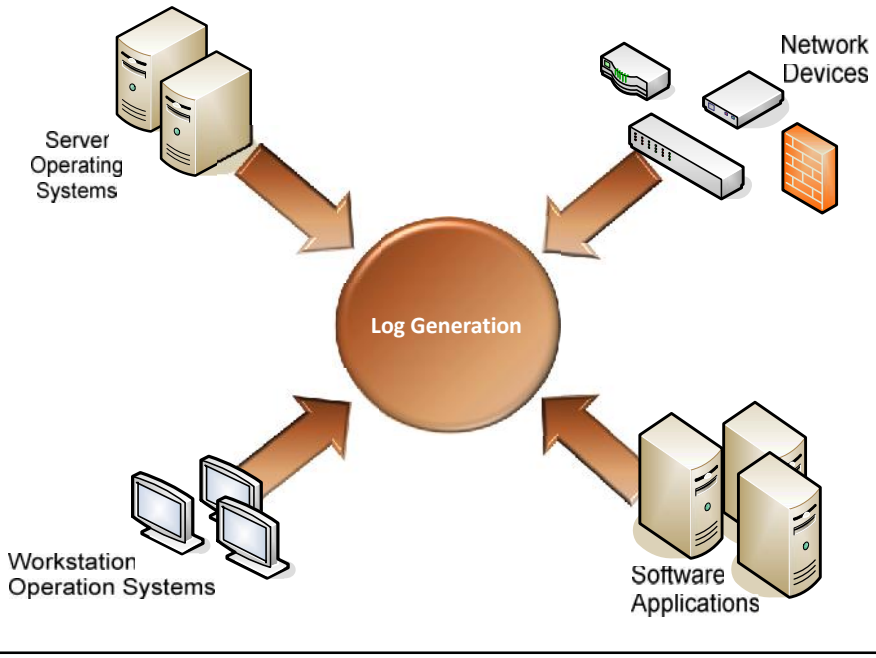
Technical Monitoring

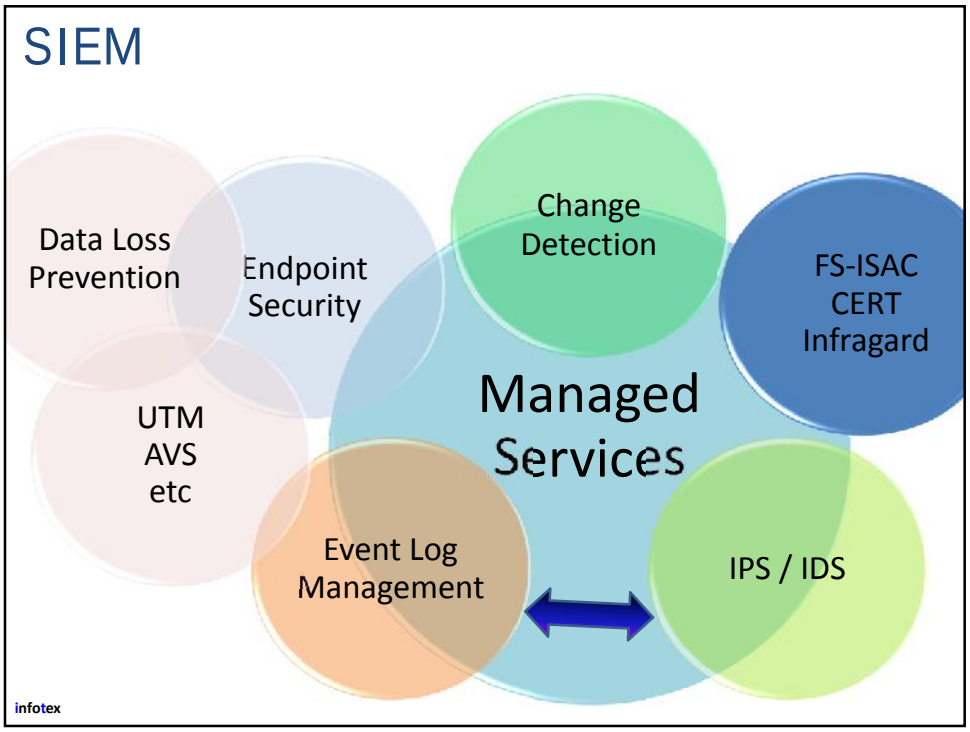
- Vulnerabilities (and Patches)
- Network Traffic
  - Scans, Malware, Policy Violations
- Event Logs (SIEM)
  - Critical Servers, Network Devices, Workstations
  - Applications
- Security Tools
  - Firewall (changes, events, vulnerabilities, etc.)
  - AVS, UTM

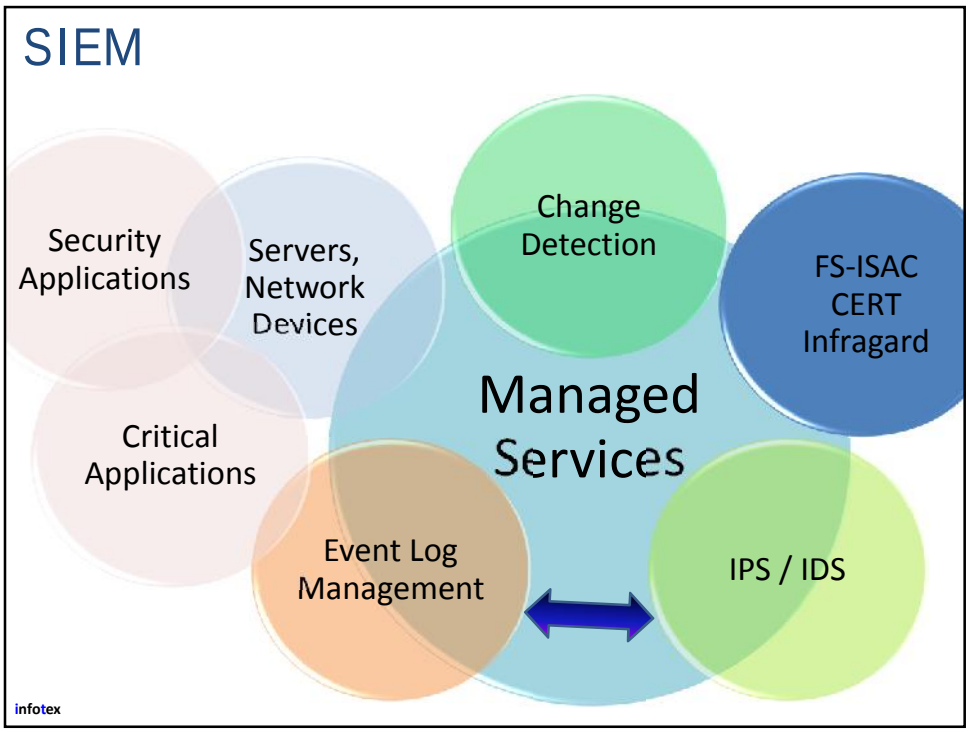
Risk Monitoring Architecture

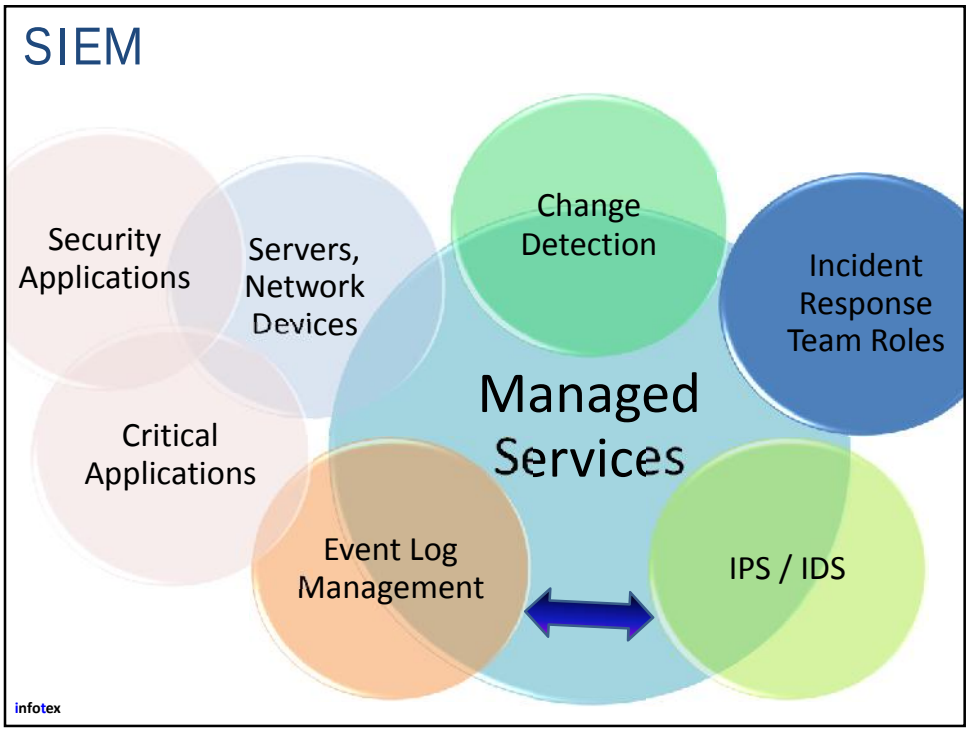


Event Log Management



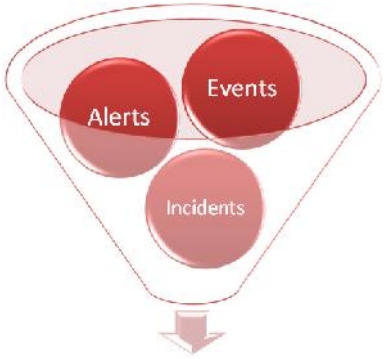

SIEM
Data Loss Prevention
Endpoint Security
Change Detection
FS-ISAC CERT Infragard
UTM AVS etc
Managed Services
Event Log Management
IPS / IDS
infotex


SIEM
Security Applications
Servers, Network Devices
Change Detection
FS-ISAC CERT Infragard
Critical Applications
Managed Services
Event Log Management
IPS / IDS
infotex



Clearing out the Noise

- About 99.9% of Alerts and Logs are False Positives
- On-average, every 20,000 logs per server per day produces 1 actionable event.



Actionable Events

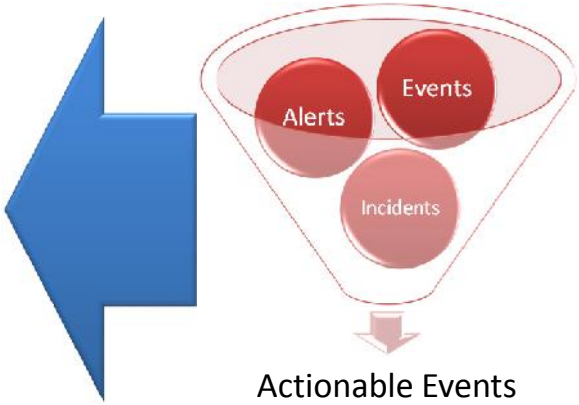
infotex

Clearing out the Noise

Real Time Response

Daily Reporting and Acknowledgment

Incident Response Team Reports



Actionable Events

infotex

Plan to start a conversation with your MSSP . . .

The NIST CyberSecurity Framework

69 of 98

control objectives are covered by a full-service MSSP engagement.

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Today's Agenda

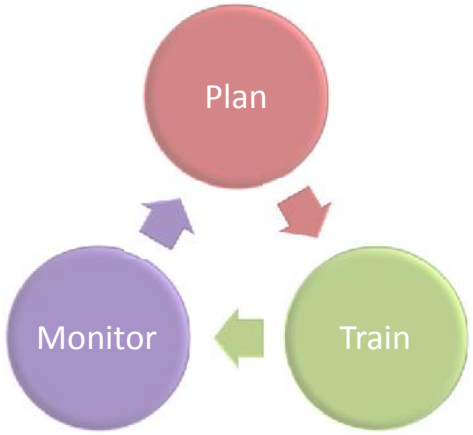
- The Workshop and the Workbook
- Incident Response Fundamentals
  - Future Compliance Frameworks
- Incident Response Program
  - Policy Considerations
  - Response Procedures
  - Customer Notification
- Risk Monitoring
  - The FFIEC Risk Monitoring Requirements
  - Anatomy of an Attack
  - Non-technical Risk Monitoring
  - The NIST Frameworks
  - Documenting a Risk Monitoring Architecture
- Putting it all to work!

Simplify IT

- Seven Steps
  1. Re-create your Incident Response Policy
  2. Develop your Incident Response Team
  3. Update our Incident Response Plan
  4. Document your Risk Monitoring Architecture
  5. Train and Re-train your IRT
  6. Test the Incident Response Team
  7. Circle Back and Review

infotex

Compliance with the FFIEC Guidelines



FFIEC FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL
Promoting uniformity and consistency in the supervision of financial institutions

Do we need another Lemons Webinar?

Updating Your Policy

1. Define an Incident (and classes)
   - Refer to a Federally Required Framework
2. Establish the Incident Response Team (or identify a committee to handle the function.)
3. Require Incident Response Team Training

infotex

Updating Your Policy

4. Require Incident Response Testing
   1. Walkthrough
   2. Tabletop
5. Simplify the Classification / Triage Process

infotex

Update Your Plan

- Adopt the NIST CyberSecurity Framework
- Focus in on the NIST SP 800-61

infotex

Risk Monitoring Architecture

- Document what you have in place.
- Have a long talk with your MSSP.
- What can you keep in-house?

infotex

I: Likelihood: *As you are reading through these "incidents," consider which ones would require disclosure. Rank the following vulnerabilities by order of their* ***likelihood of occurrence****, 1 through 10, a 1 being the highest likelihood:*

1) _____ An employee leaves various reports with NPI visible on his desk and, while retrieving a printout for a customer, the customer steals one of the reports.

2) _____ An employee accidentally sends a file with Social Security numbers and names of 1000 customers in it to a customer that had the same name as one of the bank's employees.

3) _____ A virus ends up on an employee's workstation, and it appears that the virus is sending information out of the bank's network.

4) _____ A flood in the server room causes damage to servers and an outage.

5) _____ A disgruntled customer calls the bank and convinces an employee to go to a "drive-by web page" that puts a virus on that employee's workstation.

6) _____ A customer uses weak passwords, causing the account to be compromised, and then blames the bank for the compromise.

7) _____ An employee complains about a customer on her Facebook page, and that customer finds out about the complaint through "friends of friends."

8) _____ A customer calls the bank saying he received a weird text message that said it was coming from the bank, and when he clicked on a link in that text message it didn't take him anywhere, but now him smartphone seems to run slow.

9) _____ A customer calls the bank saying she just purchased a new Eris and wants to know if the bank has a mobile app for her new smartphone. The employees at the branch have no idea which operating system (Google, Apple, RIM) the Eris runs. Neither does the customer.

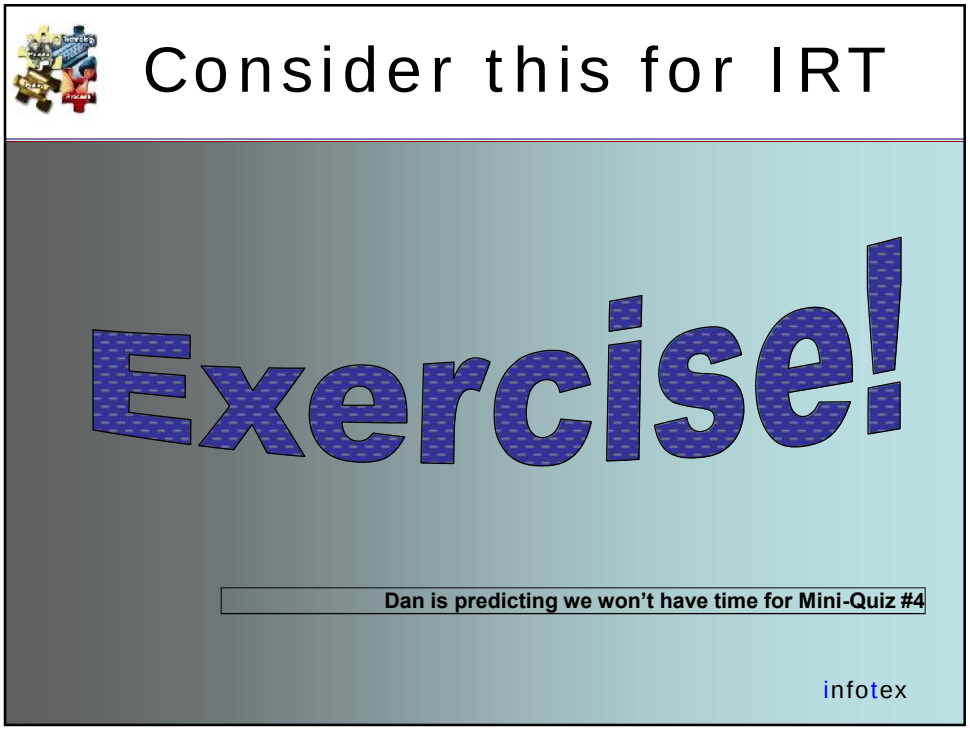
10) _____ Your MSSP informs you that a huge file with NPI in it was e-mailed out of the bank in the clear, and reports that the IP address of the sender of that file was a loan officer who just resigned.

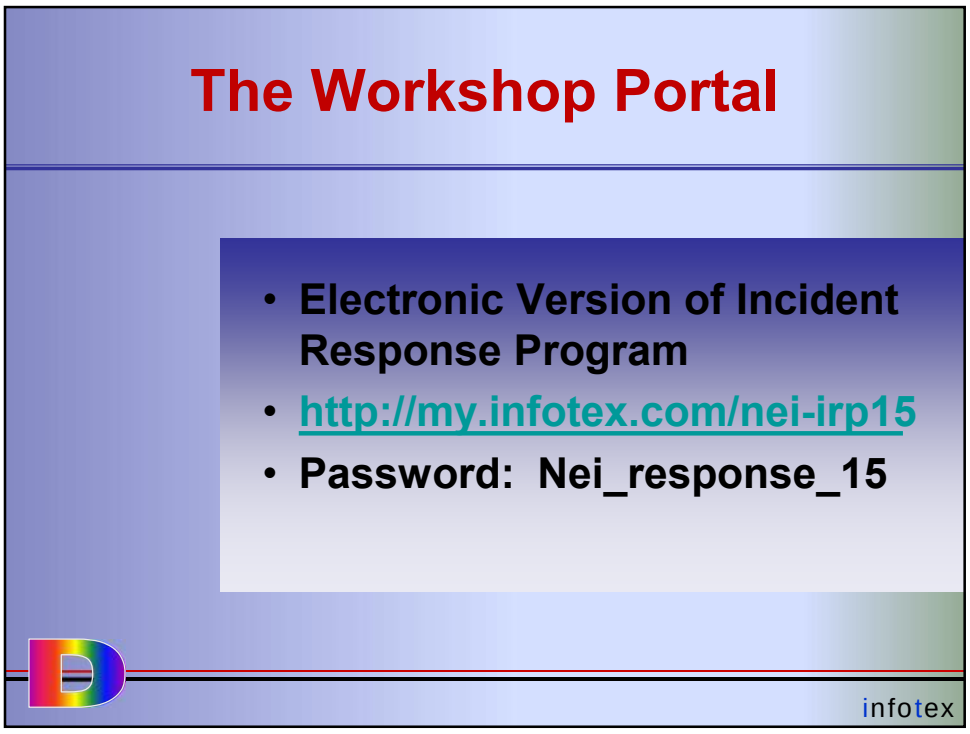
II: Disclosure, Broadcast Awareness, and the need for a Multi-disciplinary Team:

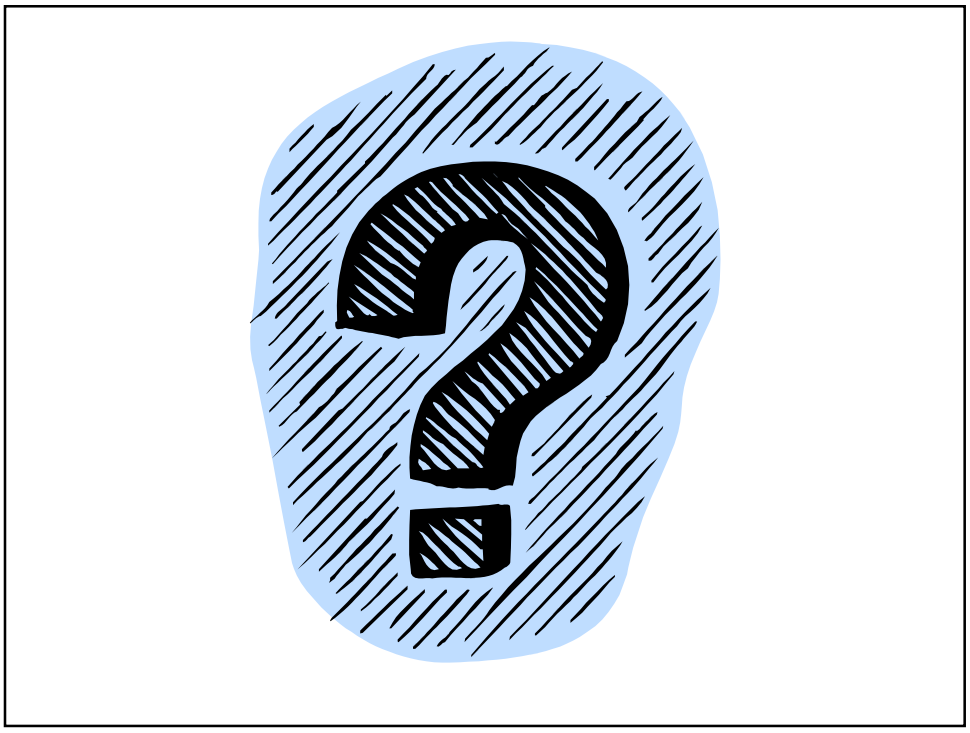
a) Which of the above "incidents" requires you to disclose to your customers? _____

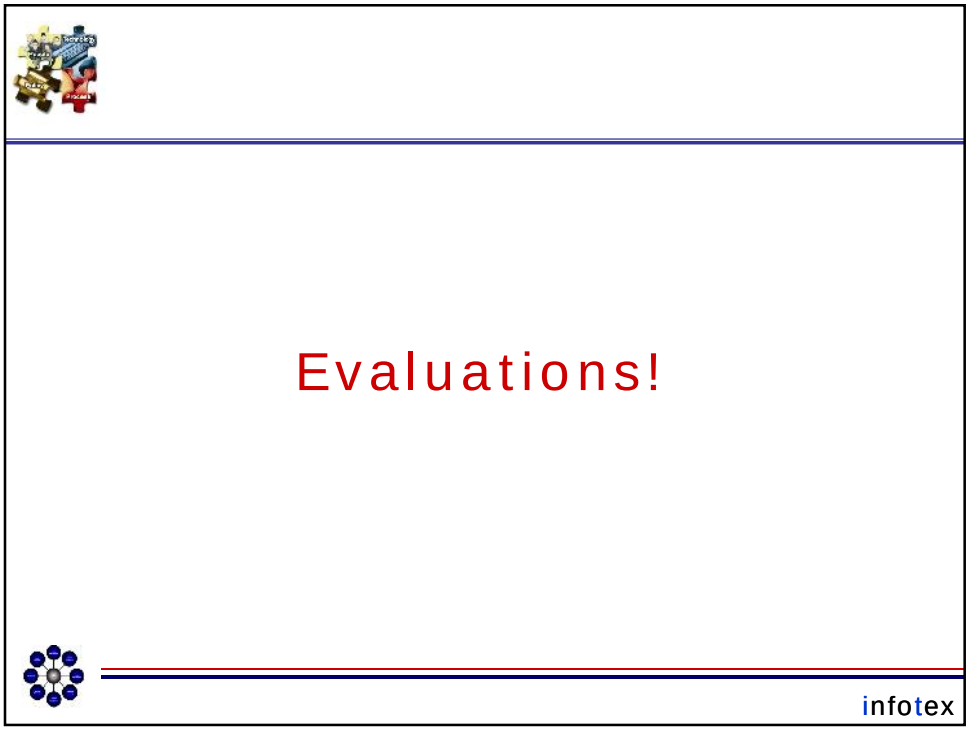
b) Which of the above "incidents" should you consider "broadcast awareness?" _____

c) Which of the above incidents might require the assistance of human resources? _____


Consider this for IRT
Exercise!
Dan is predicting we won't have time for Mini-Quiz #4
infotex


The Workshop Portal
• Electronic Version of Incident Response Program
• http://my.infotex.com/nei-irp15
• Password: Nei_response_15
infotex




Evaluations!
infotex

Thank you!

Simplify IT

- The following slides are a compilation of the “simplify IT” statements made throughout the workshop.
- We will not be going over these again in the workshop!

infotex

Simplify IT

- The first priority of any incident
  1. Containment
  2. Everything else comes second.

infotex

Simplify IT

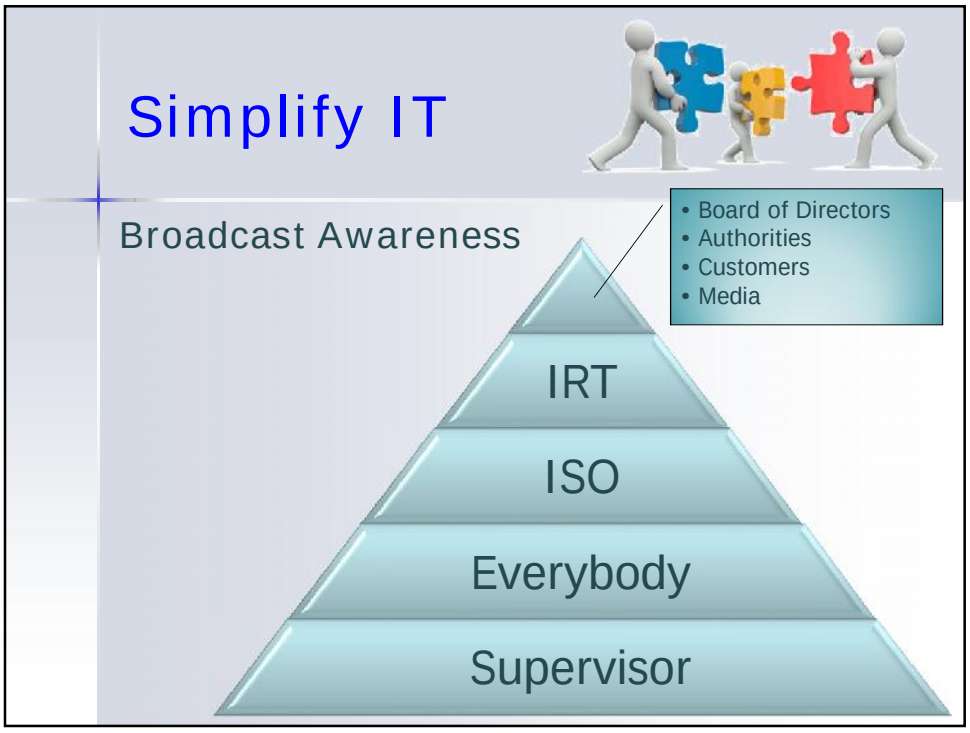
- The three steps in an incident:
  1. Broadcast Awareness
  2. Inform the Information Security Officer
  3. Assist in the Triage Process

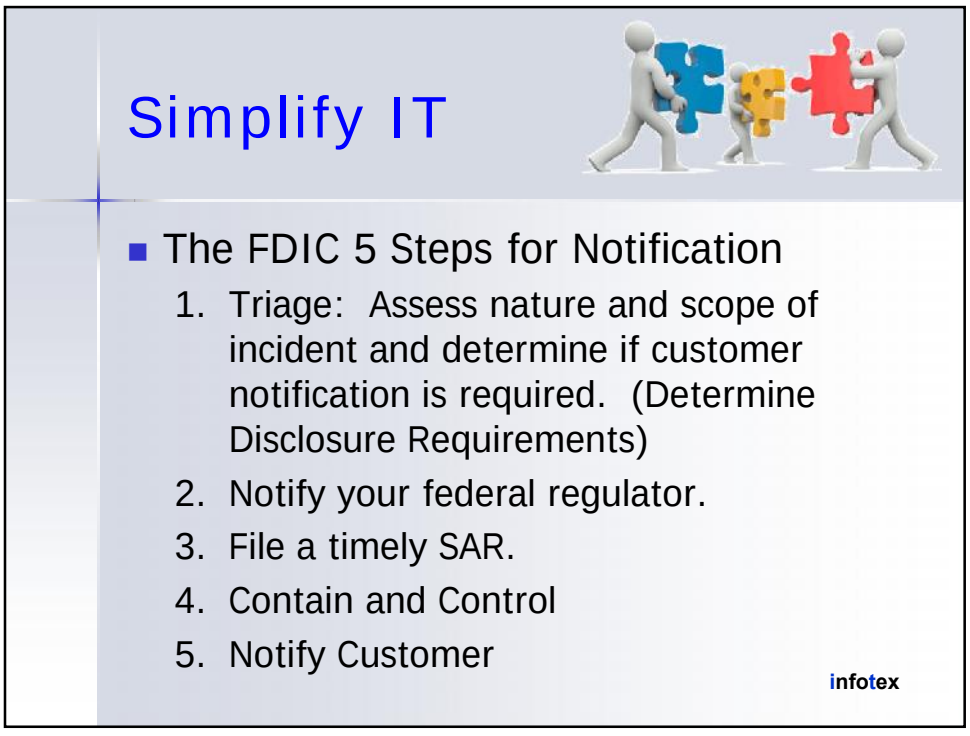
infotex

Simplify IT

- Five Types of Incident Reporting
  1. Broadcast Awareness (Real Time)
  2. Incident Log
  3. Notification
  4. Summary Reports
  5. Annual Report to the Board

infotex


Simplify IT
Broadcast Awareness
• Board of Directors
• Authorities
• Customers
• Media
IRT
ISO
Everybody
Supervisor


Simplify IT
The FDIC 5 Steps for Notification
1. Triage: Assess nature and scope of incident and determine if customer notification is required. (Determine Disclosure Requirements)
2. Notify your federal regulator.
3. File a timely SAR.
4. Contain and Control
5. Notify Customer
infotex

Simplify IT

- Triage: Determining Disclosure Requirements
  1. Detect: Broadcast Awareness
  2. Assess: Real or potential unauthorized access to customer data? Who, what, when, how, where?
     A. Has misuse occurred?
     B. Or is there a potential that misuse could occur?
  3. Respond: Classify, Document, Escalate!
     (A reasonable investigation means documentation and escalation!)

infotex

Simplify IT

- Engaging the Media
  1. Start Early
  2. Pre-train on a "generic strategy"
  3. Use the "generic strategy" to document a strategy specific to the incident, get IRT approval
  4. Choose the right person to speak to the media.
  5. Create a "media reader"

infotex

Simplify IT

- The NIST Incident Response Cycle
  1. Prepare
  2. Detect and Analyze
  3. Contain, Eradicate, Recover
  4. Post-Incident Review

infotex

Simplify IT

- Five Functions of CyberSecurity Controls
  1. Identify
  2. Protect
  3. Detect
  4. Respond
  5. Recover

infotex

Simplify IT

- Seven Steps
  1. Re-create your Incident Response Policy
  2. Develop your Incident Response Team
  3. Update our Incident Response Plan
  4. Document your Risk Monitoring Architecture
  5. Train and Re-train your IRT
  6. Test the Incident Response Team
  7. Circle Back and Review

infotex