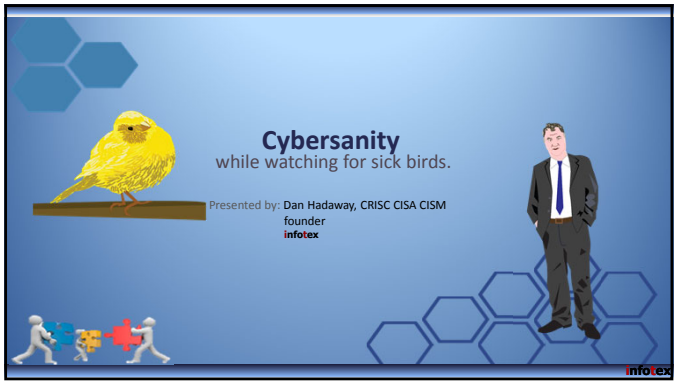

Cybersanity
while watching for sick birds.
Presented by: Dan Hadaway, CRISC CISA CISM
founder
infotex
infotex

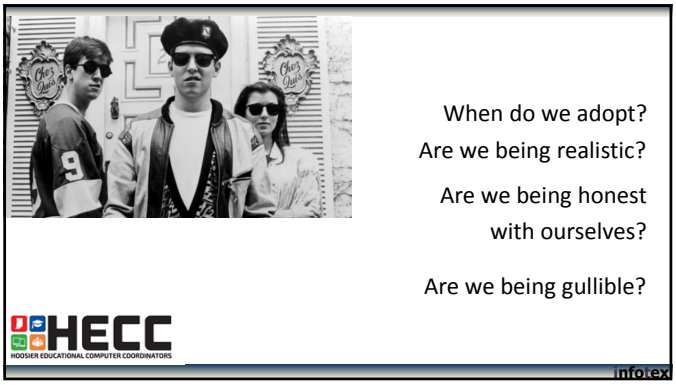
1


The New York Times
U.S. ATTACKED
HIJACKED JETS DESTROY TWIN TOWERS AND HIT PENTAGON IN DAY OF TERROR
A CREEPING HORROR
President Vows to Exact Punishment for 'Evil'

2


HECC
HOOSIER EDUCATIONAL COMPUTER COORDINATORS
infotex

3



When do we adopt?

Are we being realistic?

Are we being honest with ourselves?

Are we being gullible?

HECC
HOOSIER EDUCATIONAL COMPUTER COORDINATORS

infotex

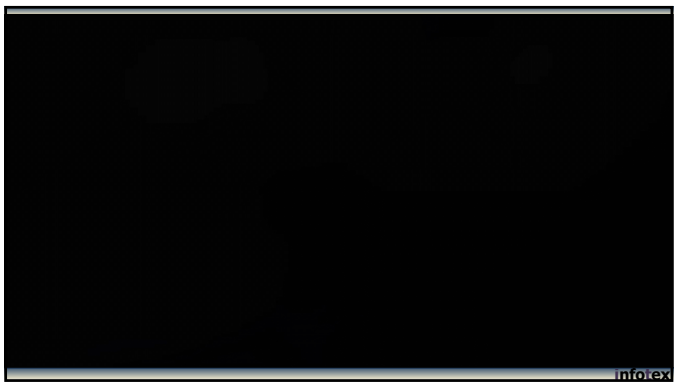
4

Famous Last Words

"Our patch management system worked okay."

infotex

5



infotex

6

Famous Last Words

"Our patch management system works okay."

"We can handle this on our own!"

infotex

7

Lone Ranger Approach

infotex

8

Famous Last Words

"Our patch management system works okay."

"We can handle this on our own!"

"We have no time to test!"

infotex

9

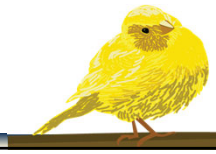
Sharpening the Saw

HECC
HOOSIER EDUCATIONAL COMPUTER COORDINATORS

infotex

10

The Canary in the Coal Mine



11

Risk Management

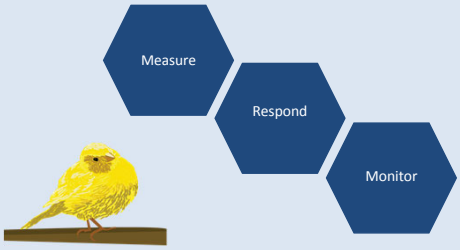
Measure Respond

Monitor

infotex

12

Risk Management Metaphorically



infotex

13

Risk Management Metaphorically

infotex

14

What do we monitor?

- Our risk response:
  - Transferred Risk
  - Risk Mitigation
  - Accepted Risk
    - Threats Exploiting Vulnerabilities

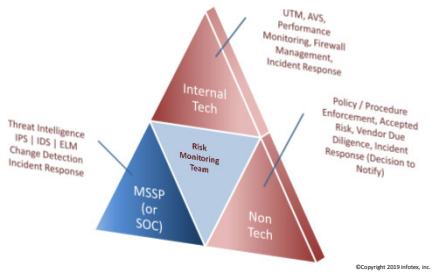
infotex

15

Monitoring
Accepted Cyber Risk
equals
Looking for Threats Exploiting Vulnerabilities

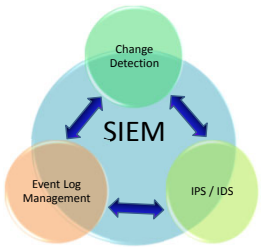
16

SIEM: Three Teams Working As a Team



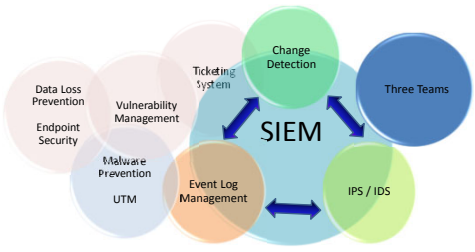
17

The SIEM Architecture using an MSSP



18

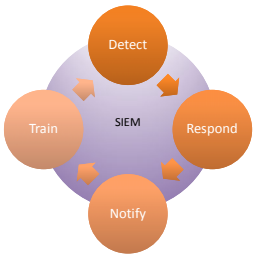
The SIEM Architecture using an MSSP



infotex

19

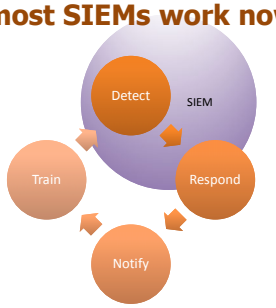
Incident Response Process (according to NIST)



infotex

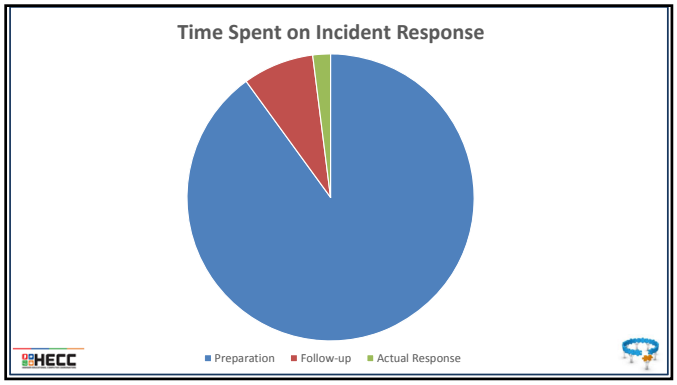
20

How most SIEMs work now . . .



infotex

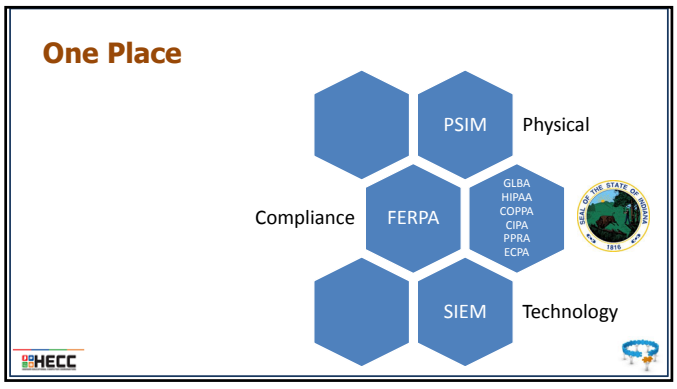
21


Time Spent on Incident Response
Preparation
Follow-up
Actual Response

22


Incident Log
Response Wizard
Active Incident
Tool Library
Standard Agenda
This Month Agenda
PLACE
Reports Repository
Ticketing System
SIEM Inputs
Journal
©Copyright 2017 infotex, inc.

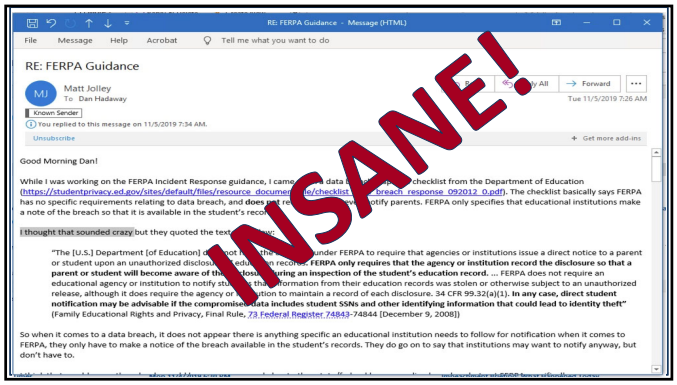
23


One Place
PSIM
Physical
Compliance
FERPA
GLBA
HIPAA
COPPA
CIPA
PPRA
ECPA
SIEM
Technology

24


Insanities
INSANE!
PSIM
Physical
FERPA
GLBA
HIPAA
COPPA
CIPA
PPRA
ECPA
SIEM
Technology
infotex

25


INSANE!
RE: FERPA Guidance - Message (HTML)
RE: FERPA Guidance
Matt Jolley
Dan Hadaway
Good Morning Dan!
While I was working on the FERPA Incident Response guidance, I came
checklist from the Department of Education
(https://studentprivacy.ed.gov/sites/default/files/resource_
). The checklist basically says FERPA
has no specific requirements relating to data breach, and does
notify parents. FERPA only specifies that educational institutions make
a note of the breach so that it is available in the student's
I thought that sounded crazy but they quoted the
"The [U.S.] Department [of Education]
under FERPA to require that agencies or institutions issue a direct notice to a parent
or student upon an unauthorized
FERPA only requires that the agency or institution record the disclosure so that a
parent or student will become aware of the
during an inspection of the student's education record.
FERPA does not require an
educational agency or institution to notify
information from their education records was stolen or otherwise subject to an unauthorized
release, although it does require the agency or
tution to maintain a record of each disclosure. 34 CFR 99.32(a)(1). In any case, direct student
notification may be advisable if the compromised
data includes student SSNs and other identifying information that could lead to identity theft"
(Family Educational Rights and Privacy, Final Rule, 73 Federal Register 74843-74844 [December 9, 2008])
So when it comes to a data breach, it does not appear there is anything specific an educational institution needs to follow for notification when it comes to
FERPA, they only have to make a notice of the breach available in the student's records. They do go on to say that institutions may want to notify anyway, but
don't have to.

26


In search of guidance
Compliance pressure from three directions:
Department of Education (FERPA)
Health and Human Services (HIPAA)
Federal Trade Commission (GLBA)
HECC

27

In search of guidance

- Compliance pressure from three directions:

Student Information

Health Information (ePHI)

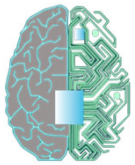
Financial Information (PII)

infotex

28

infotex hecc portal

- **Free Tools:**
  - Posters (free at posters.infotex.com)
  - Compliance Resources
  - Boilerplates*
  - Incident Response Program Audit Checklist
- **my.infotex.com\freetools-hecc19**



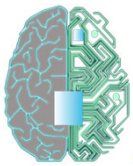
**Note that boilerplates are imperfect starting points!*

infotex

29

Laws and Guidance

- Compliance Resources:
  - FERPA Guidance Summary (for IT Governance as a whole)
  - FERPA Guidance Summary – Incident Response
  - FERPA Incident Response Checklist
  - The actual State Law (Indiana)
- **my.infotex.com\freetools-hecc19**

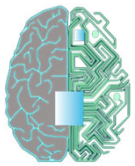


infotex

30

Free Boilerplates!

- Technology Risk Monitoring Policy
- Technology Risk Monitoring Plan
- Incident Response Program Checklist



- https://my.infotex.com/testing-your-siem/
- **my.infotex.com\freetools-hecc19**

Note that boilerplates are imperfect starting points!

infotex

31

The Cusp

External communications to parents, teachers, faculty, administration, law enforcement and/or the media must be reviewed by the Technology Risk Monitoring Team, and presented to Management for approval prior to releasing it to the public. Specifically:

Disclosure Incidents: [Indiana Law (Indiana Code section 24-4.9) / Applicable Local Laws] requires notification of parents, students, and/or faculty in the event of a data Best practice requires a five step process to be completed in order to respond to Disclosure Incidents:

1. Contain and Control the Incident
2. Triage: Assess nature and scope of incident and determine if notification is required. (Determine Disclosure Requirements) Consider enlisting the help of the MSSP, PTAC, forensics firms (approved by insurance), legal counsel and/or the insurance agents.
3. Consider notifying the State's Attorney General's Office. Consider notifying the Family Policy Compliance Office (FPCO).
4. If there is a potential for misuse: Notify Parents, Students, and Faculty. If not, document!
5. Conduct a post-incident review (Post-Mortem Review)

State Law defines "personal information" as:

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

infotex

32

33

Hint:

You walked past it this morning!

infotex

34

35

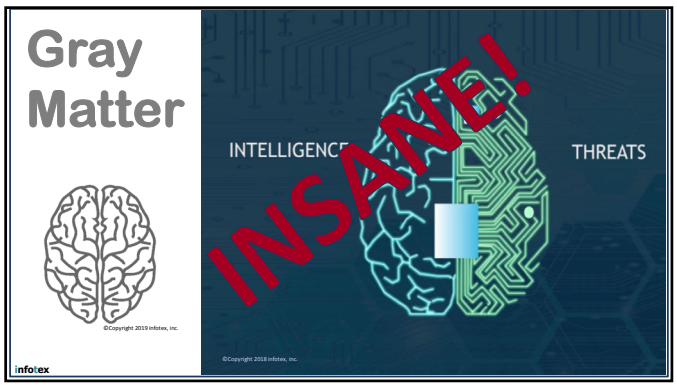
When we don't monitor

- Likelihood increases
- Reputation decreases
- Change Management
- Denial of Service (DoS)
- Compliance Deficiencies

- Unauthorized access

infotex

36



37

Dead Birds

- Is your mouse cursor moving and you're not touching your mouse?

infotex

38

Dead Birds

- Does every workstation have the same screen – a countdown timer with Bitcoin instructions?

infotex

39

Dead Birds

- Do you have a vendor due diligence process?

infotex

40

Monitoring
Risk Transference

HECC

41

MSSP Due Diligence

- Do not "host" Student data, PII or NPI, ePHI
- Do not even have "access" to sensitive data.

- But -

- Persistent Connection to the Internal Network
- A breach of an MSSP could lead to a breach of the bank

infotex

42

MSSP Due Diligence

- Specific Service Level Agreements
  - Guaranteed Response Time
  - What is a "response?"
- FFIEC Examination Program (in banking)
- Third Party Audits
  - Vulnerability Assessments, Pen Tests
  - Social Engineering Tests
  - Network Configuration Audits
  - Non-technical Controls Review
- Adequate Insurance
- Quality Controls (see next slide)

infotex

43

MSSP Quality Controls

infotex

44

MSSP Due Diligence

- Test Your SIEM
  - That you can test should be part of your agreement.
  - You can implement many SIEM testing processes internally.
  - https://my.infotex.com/testing-your-siem/

INSANE!

infotex

45

More Insanities

46

47

Security Culture

- Appropriate Awareness in All Directions
- Self-reporting is encouraged.
- Board minutes reflect IT Governance as a priority.

48

49

Dead Birds

- Do you have an incident response program?

50

Insane Incident Response

EQUIFAX

- No notification for many weeks.
- Stock sold after incident knowledge, before notice.
- An attempt to deceive customer base
  (Agreement not to sue in the fine print on free credit monitoring offer)
- A drip drip drip parade of breach news.

51

What to avoid . . .

infotex

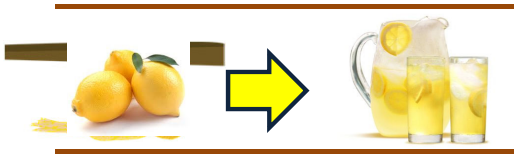
52

What to avoid . . .

infotex

53

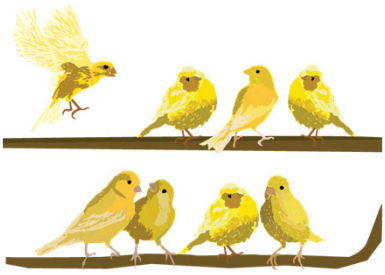
Sane Incident Response



infotex

54

Write this down.



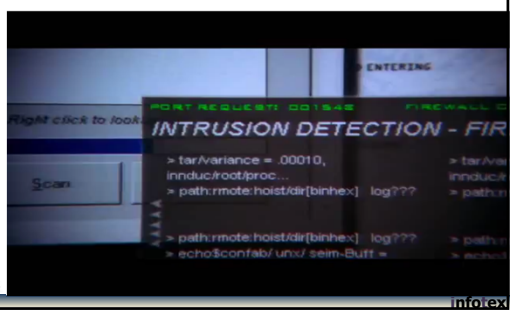
infotex

55

infotex

56

Are we as gullible now as we were in 2004?



infotex

57


That Hacks Look Like This
INSANE!
Yet in 2019 we brace for the cyber attack, while pretext callers go ignored.
infotex

58


You Can Pull Up A Hacker's Profile
INSANE!
NCIS 2 IDIOTS 1 KEYBOARD
Which is like, in 2019, school corporations acting like they're going to be able to handle threat intelligence on their own.
infotex

59


That You "Hack Back."
INSANE!
Whereas in 2019 schools think that proactive arrangements with forensics firms may be a waste of money.
infotex

60


Four hands are better than two
NCIS 2 IDIOTS 1 KEYBOARD
INSANE!
Analogous to 2019, when a Technology Coordinator is convinced he can build his own network monitoring approach.
And monitor text messages 24x7?
infotex

61


INSANE!!
infotex

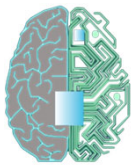
62


The Sickest Bird
infotex

63

infotex OER - Places to Go!

- https://my.infotex.com/testing-your-siem/
- posters.infotex.com | p7.infotex.com
- movies.infotex.com
- schools.infotex.com
- **my.infotex.com\freetools-hecc19**



Note that boilerplates are imperfect starting points!

infotex

64

Evaluations

HECC
HOOSIER EDUCATIONAL COMPUTER COORDINATORS

infotex

65

Questions

infotex

66

67