infotex

EDUCATIONAL OPPORTINITIES

talks.**infotex**.com

webinars.**infotex**.com

Our Clients Are Cybersecurity Superheroes

And our training programs respect their busy schedule, ensure their management team feels that their time is well-spent, and establish the importance of Confidentiality, Integrity, and Availability . . . not only at work . . . but also, at home and in our community.

Free Training Resources

- movies.**infotex**.com
- webinars.**infotex**.com
- posters.**infotex**.com
- m7.**infotex** com
- blog.**infotex**.com

Educational Events

- Speakers
- Conference Moderators
- Panel Discussions
- Talks
- Presentations
- Key-notes
- Technical and Non-technical

Testing Services

- Penetration Testing (technical, nontechnical, hybrid)
  - Perimeter Attacks
  - Orchestrated Attacks
  - Social Engineering
  - Public Presence Reviews
  - Ongoing Pretext Calls, Pretext Calling
  - Phishing, Phone Phishes
  - Physical Breach Attempts
- Security Awareness Posture Assessments
- Endpoint Audits

Awareness Exercises

- Incident Response Tabletop Tests
- User Awareness Training
- (and custom movies)
- Customer Awareness Training
- (and custom movies)
- Lunch and Learns
- Board Basic Training
- Custom Day-long Workshops
- Technical Training

FREE BOILERPLATES FOR ALL CLIENTS!

boilerplates.**infotex**.co

24x7x365

Managed Security Operations Center

infotex Managing Technology Risk my.**infotex**.com (800) 466-9939

infotex

EDUCATIONAL OPPORTUNITIES

talks.**infotex**.com

webinars.**infotex**.com

Awareness – a key control

While as auditors and MSSPs we cannot make changes to your system, we assist with the execution of three interactive tactics to establish what we've come to call "Awareness," a critical control in IT Governance. By establishing this control at the board, management team, technical team, user, vendor, and customer levels, we ensure a balanced, risk based approach to cyber and information security. The most educated cyber-expert still clicks on links, due to a lack of activation, while users who know the policy violate it, due to a lack of motivation (not understanding why the control is in place.)

Education

We have seen that humans, often by clicking on a link, become the weakest link. By focusing resources on educating, motivating, and awareness activation, we create a smoother compliance path, putting everybody on the same page in a manner commeasure with risk and complexity. Through movies, webinars, seminars, day-long workshops customized to the Client, Incident Response Testing and Training, and many other approaches, we help our Clients overcome the weakest link through Education. Our policy and procedure boilerplates are free to all Clients, as are at least 12 webinars and movies per year.

Motivation: Realizing Why

Management, Board, Technical Team Awareness

We have mastered the art of opening the eyes of management team members, connecting the three teams of a security information event management process, through the use of the FFIEC Required incident response methodology: Training, Test Planning, Tabletop Testing, and Post-Mortem Review.

Custom Training Movies

Prior to 9/11, we did not remove our shoes at checkpoints. But now we know why, and thus we comply. We produce custom movies to train employees and customers. Our custom training services, from comedy-hours to lunch and learns, seminars, day-long workshops, webinars and movies, align with compliant strategy for training your board, management team, technical team, employees, vendors and customers.

Activation

We have caught the ISO that hired us in social engineering test, several times in our twenty-plus year history. This means that the most educated and motivated person is still not aware unless their awareness is ACTIVATED. We must be put on guard, and remain there, to be vigilant. Our free awareness posters are meant to remind employees and customers of their role in our safety.

Awareness Testing

In 2002 we conducted our first penetration test that orchestrated physical, logical, and social engineering tactics. In those early days, we would find ourselves hiding under conference tables, in dumpsters, and texting pictures from server rooms. All this time, we always noticed an ironic truism . . . . people will click on links when they think they may be malicious, but if they think it could be a test, they are completely vigilant. Mindfulness increases when we know there is a high likelihood that the next phone call, the next email, the next vendor visit, could be a test.

We have mastered the physical breach attempt, the pretext call, and the orchestrated penetration test. We have successfully plugged flash drives into servers in "bullet proof" data centers. But we also know the "capture the flag" tactic is not always the best approach. We have designed methodologies and metrics focused on incremental improvement, using tactics aligned with your overall strategy. Our approach includes posture interviews, endpoint audits, and comprehension exercises.

Incident Response Tabletop Tests

In twenty plus years of direct experience working with financial institutions, hospitals and others wanting to be secure, the one control that covers the most ground, the one tactic that achieves the best awareness, in our opinion, is the incident response tabletop test. This one exercise, if designed and executed right, creates a team approach to not only incident response, but governance as a whole.

We had to cancel our first security workshop, scheduled for 09/12/2001. Since then we developed these resources:

webinars.**infotex**.com	movies.**infotex**.com
posters.**infotex**.com	testing.**infotex**.com
board.**infotex**.com	audits.**infotex**.com

24x7x365

Managed Security Operations Center

◆▶ **infotex** ◆▶ Managing Technology Risk ◆▶ my.**infotex**.com ◆▶ (800) 466-9939 ◆▶