Security Awareness Training

Introductions

- Describe your firm, background, and how are you part of the security program at your firm?
  - Mark Brophy: Director of Information Technology, Rogers Townsend & Thomas
  - Gil Danieli: Manager of Information Security, Schulte, Roth & Zabel
  - Adam Carlson: Security Solutions Manager, IntApp

Why Awareness Training?

- Lots of possible security investments
- Awareness training requires coordination/cooperation
- Not always in the comfort zone of IT
- *What was the driving factor for you and your firm?*

Some Good Reasons

- 33% of breaches are the result of user negligence
  - Ponemon Institute 2013 Breach Study
- Individuals increasingly being targeted
  - “Spear-phishing most common form of attack” – Special Agent Eric Brelsford, LegalSEC Keynote 2013
  - “Spear-Phishing Email: Most Favored APT Attack Bait” – Trend Micro 2012 Report
  - “Law Firm Falls Victim to Phishing Scam, Sued by Bank”, April 2013

How Did You Secure Buy-In?

- Legal may be the most expensive industry to train
  - 20 lawyers at $500/hour = $10000/hour
- Lawyers don't like to be told what to do
- Management may still see security as an IT problem
- *What was the persuasive reason for your firm's management?*

Management-Level Concerns

- Failure to adhere to industry best practices
- Third-party assessment
- Clients (RFPs, Audits, other)
- Regulatory reasons
  - HIPAA – Compliance deadline in September 23, 2013
  - State breach notification laws
- Malpractice carrier rates/incentives
- Ethical obligations - ABA Rule 1.1 and 1.6
- Examples of past incidents and their clean-up costs

Who Did You Partner With?

- Information security extends beyond IT
- Many firm members have an interest in effective security
- IT not always seen as authoritative
- *Who did you involve in your awareness planning?*
- *What role did they or will they play?*

Key Security Stakeholders

- Firm Administrator/CEO
- Executive Committee
- Operating Committee
- Technology Committee
- Managing Partner
- Risk Partner
- Risk Manager
- Practice Group Leaders
- Information Systems
- Records/Accounting
- Human Resources
- PR/BD Officer

How Did You Select Content?

- Unlimited ways to lose data and cause problems
- Very tight time constraints
- *How did you choose your curriculum?*
- *Who was involved in that decision?*

Make It Contextual

- Check the box
  - HIPAA requirements, client expectations
- Use relevant examples
- Make it personal
  - Consider tips that will help them at home
- Don’t reinvent the wheel
  - Lots of free resources

How Is It Being Delivered?

- Live training can be more impactful but logistically hard
- Recorded training is convenient but hard to track
- Posters and handouts can also be leveraged
- *What format did you decide to use?*
- *Are you offering ongoing training opportunities?*

Content/Delivery Factors

- Vendor solutions often have predetermined content
- Recording videos in-house may be tough
- CLE credit requirements vary by state
- May need something that can track participation
- Law firm examples/live demonstrations

What About Staff?

- Handling much of the same data
- Working on the same systems
- Not bound by professional responsibility obligations
- *Are you training law firm staff?*
- *Is there any difference in the approach/content?*

Is It Worth It?

INDUSTRY VIEW

Why you shouldn't train employees for security awareness

Dave Aitel argues that money spent on awareness training is money wasted

» 86 Comments Share 69 +1 Like 118 More

By Dave Aitel, Immunity Inc.

Why security awareness training is a waste of time

Cory Doctorow at 9:28 pm Wed, Mar 27, 2013

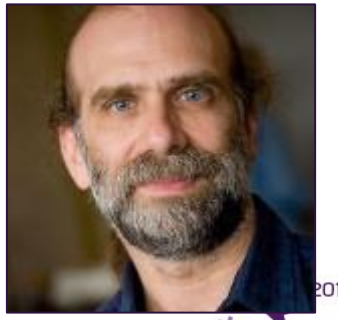
24 Like 119

Bruce Schneier presents a very cogent and convincing argument that "security awareness training" is a waste of money -- specifically, because the benefits of "security" are intangible, while the benefits of getting your work done are apparent.

— FEATURED —

THE LATEST

Free stream: The Sou
Family soundtrack of
cult psychedelia



2013

the catalyst

Yes, It Is

- Stopping 90% of the attacks is still something
- Training is about more than spear-phishing
- Creating a culture of security isn't measurable
- Included in every major security standard for a reason

Every Road Has Its Bumps

- *What aspects of your Security Awareness Training do you think has been successful?*
- *How are you measuring success?*
- *What has been the most challenging aspect?*

Free Content Sources

- SANS - http://www.securingthehuman.org/resources
- MindfulSecurity.com
- US-CERT.Gov – Protect Your Workforce Campaign
- NIST Special Publications 800-50/NIST 800-16
- Dept. of Homeland Security – Stop.Think.Connect. Campaign
- Educause Cybersecurity Awareness Library

Looking Forward

- Mark
- Gil
- Adam

Questions?