TRAINING

Security Awareness Program Design

Description

Security Awareness is well-known for being the “best bang for the buck” out of all the risk mitigation techniques, but is it really?

Security Awareness programs can be effective, if they are designed with adult learning techniques, allowing retention and behavior change. They must also be complete and address all roles the employees have, ideally leading to a mature security culture in your organization.

Programs that focus only on Phishing for instance, are important, but only when used as PART of a complete program that addresses everything from buy-in to remediation and cover all Social Engineering topics, such as Social Media and Mobile Devices. Many programs that do not use adult education techniques and neuroscience fail to achieve behavior change and can even make things worse.

Once employees start to have a negative impression about information security, feel helpless, or begin to consider remediation as punitive, great damage has been done to the security culture and this can be difficult to reverse.

The intent of these programs is to “inoculate” employees against both purposeful and accidental triggering of security threats to your organization. Employees will come away empowered to self-sustain a competent level of security awareness for protection of organizational property, as well as personal identity security. These programs are designed by Cadre’s experts to avoid the problems that arise with “cookie cutter” classes. Cadre will create an efficient method by which all employee roles and classes pull from a ‘menu’ of Security Awareness topics, providing useful and meaningful information to each employee.

Once employees have bought into the importance of Security Awareness, continuing education programs can keep the culture’s maturity sustained through programs such as class updates, webinars, videos, micro learning, phishing exercises, games, and events.

Does Cadre teach the classes, write the courseware, design the program or implement the program?

Cadre can do it all. We are here to take the burden off you. We can help design and implement, and once your program is set up and working, we can continue to play the same role, train your team to take over, or even combine forces expanding the program.

The courses can be tailored to meet all major compliance standards, including: HIPAA, PCI-DSS, GLBA, FISMA, NIST 800-53, ISO/IEC 27002, Red Flags, NERC CIP, CobiT, GDPR and U.S. State Privacy Laws.

1-Hour Introduction to Security Awareness

This 1-hour fun and energetic introduction defines security awareness, explains why it is an important skill for all employees, and presents some of the key components of security awareness training and program design. This program is designed to generate buy-in for the business value inherent in having a good security culture. Audiences can be decision makers, organization leaders, stakeholders, or anyone that can benefit from knowing what good Security Awareness is and how to implement it.

Security Awareness Classes

No two organizations are the same and likewise when it comes to security awareness training. These courses use a menu of cybersecurity topics and case studies to adapt the content to the needs of attendees. Each class incorporates the adult learning and neuroscience principles with the latest information available in the cybersecurity field. The result is effective learning retention and the skills to better combat social engineering exploits.

Sample Menu of Topics Used to Create Course Agendas:

The following is a short partial list of some of the topics used to customize content for EVERY role in your organization from temporary workers to the CEO and the Board of Directors.

Keeping up with the Bad Guys

- What is “Security Awareness” and what does it have to do with me?
- Understanding the value of security controls
- How to stay on top of security exploits "without even trying"
- Email and browser hygiene

Understanding Cybersecurity

- Are humans included as part of "Defense in Depth" policy?
- Governance, Retention Policy and Metadata
- Mitigation and Deterrents
- Hashes, One-way Encryption, Single Key and Two Key Encryption
- Cyber Attacks and Exploits
- Social Engineering
- Hoaxes

Personal Privacy and Why it is Important to Both You and Your Employer

- Is what is good for the goose, good for the farmer?
- Keeping your personal life out of work and vice versa

Cloud Migrations and Cloud Resources

- What is "the Cloud" and how do I know if it is secure?
- Cloud data location matters
- Who controls information in the cloud and what are my responsibilities?
- Data Encryption and protection

Metrics that Matter; is Security Awareness Working?

- Metrics to evaluate Security Awareness, Behavior Change and Culture Maturity
- Situations where Phishing click through rates can provide incorrect or misleading metrics
- How to tell if remediation techniques are working or creating additional issues

Policies, Compliance and Due Diligence

- Special topics for C-Level employees and Directors
- Why you can’t outsource your Due Care
- Due Diligence for suppliers, contractors, partners and 3rd parties
- Information security as a business process and competitive advantage
- Understanding compliance and the role of policies
- Handling internal and external communications during an incident
- Keeping conflicts from making a security incident worse
- BYOD problems and mitigation techniques
- Continuing your security education

Case Studies and Discussions:

- Case Study Analysis: Social engineering
- Case Study Analysis: Ransomware
- Case Study Analysis: USB memory sticks and removable devices
- Case Study Analysis: Mobile applications
- Case Study Analysis: Bluetooth scams
- Case Study Analysis: Wi-Fi exploits
- Case Study Analysis: Evil twins
- Case Study Analysis: Signs of fake and real malware infection
- Case Study Analysis: When and how to get help
- Case Study Analysis: Why are employees going around security controls
- Case Study Analysis: Cloud security exploitations and breaches

Audience

These courses can be designed for all roles in your organization, from the CEO and Board of Directors, to your IT department and every employee. IT roles will often have a highly technical focus and decision maker roles are likely to have a business process focus.

1-Hour Introduction	$450 List Price
Security Awareness Program Design and Development	Rates are scaled to give the best value for the size and needs of your organization.

** Quantity discounts available upon request.*