ERMProtect
Cybersecurity Solutions

Information Security & Training

UNDERSTAND THE UNKNOWN

GUIDE TO DEVELOPING AN EFFECTIVE INFORMATION SECURITY AWARENESS PROGRAM

ERMProtect | 800 S Douglas Road, #940, Coral Gables, FL 33134 | www.ermprotect.com

Table of Contents

Introduction 2

Objective 2

Framework 2

Roles and Responsibilities 2

Regulations and International Standards 3

Key Success Factors 3

Reference Materials 4

Steps to Develop an Information Security Awareness Program 4

1. Evaluate Current State 4
2. Develop an Information Security Awareness Program 5
3. Implement the Information Security Awareness Program 7
4. Maintain the Information Security Awareness Program 7
5. Measure and Track Performance Metrics 7

Appendix A 8

Appendix B 9

Introduction

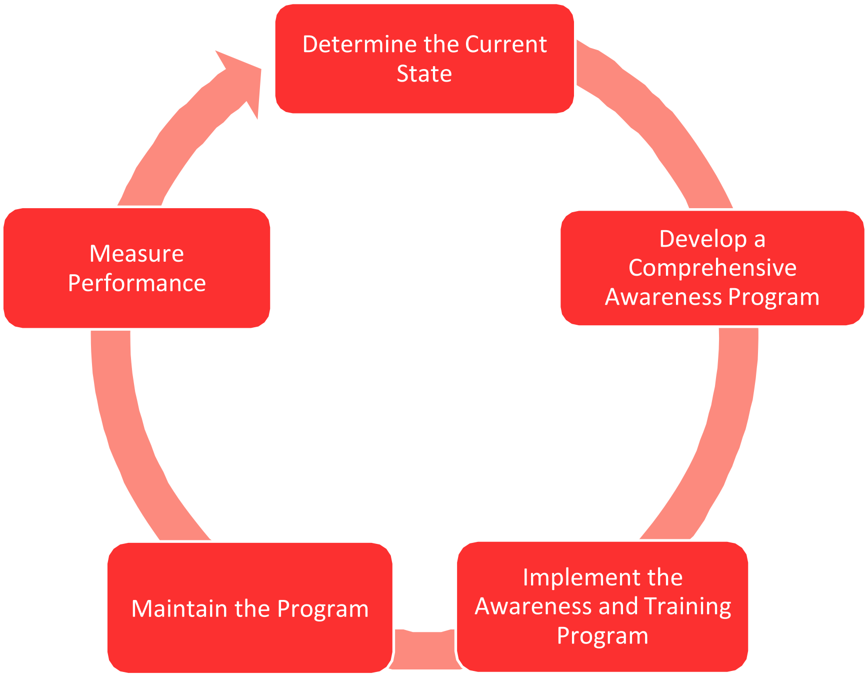
Objective

The human element has long been regarded as the weakest link in cybersecurity. But there are ways to significantly reduce your risk. In fact, with cyberattacks becoming an everyday occurrence, it is more critical now than ever for your employees to become human firewalls. Hackers are keenly aware that human error is the low hanging fruit they can exploit to gain unfettered access to even the most sophisticated technical infrastructures. Technology alone cannot be the solution.

The primary objective of an Information Security Awareness Program is to enable employees to thrive in a culture where being cyber-aware is the norm and protecting themselves and their organization is second nature. When an organization engrains information security into the culture, the threats of today, and the emerging ones of tomorrow will not look as menacing anymore.

Framework

An Information Security Awareness Program Framework helps an organization design and develop a robust Information Security Program, as well as measure its impact. Below is an example of a framework.


Determine the Current State
Develop a Comprehensive Awareness Program
Implement the Awareness and Training Program
Maintain the Program
Measure Performance

Roles and Responsibilities

It is important that organizations clearly articulate roles and responsibilities within the program. In this way, organizations ensure that accountability is unequivocally allocated. It important to have representation from all departments and functional units with diversity in individual roles and hierarchical levels. This healthy mix of individuals from across the organization should then participate in the development, implementation and tracking of the Information Security Awareness Program.

Examples of individuals who could be included:

- Senior Executives
- Information Technology Management
- Information Security Management (e.g. Chief Information Security Officer)
- Information Security Administrator
- Human Resource Management
- Legal Management
- Risk Management
- Product Development and Deployment Management
- Sales and Marketing Management
- Data Owners
- End Users

Regulations and International Standards

U.S. regulations, while critical for compliance reasons, often provide a foundation atop which cybersecurity efforts can be implemented. Similarly, international standards provide a great baseline to address cybersecurity threats from a global perspective. Organizations should identify the regulations applicable to them and research widely acclaimed and accepted international standards so that they may be incorporated into the Information Security Awareness Program.

Some examples of regulations and standards include:

- GLBA
- FACTA
- HIPAA
- HITECH
- FERPA
- FISMA
- SOX
- New York DFS 500 Regulation
- GDPR
- ISO 27001
- PCI DSS
- NIST

Key Success Factors

Several key factors go into building an effective Information Security Awareness Program. Some examples include top management support, diverse and cross-functional involvement, content that targets diverse audience groups, use of multiple training tools, unique training materials that trigger engagement, continuous communication, and measurable success criteria.

Reference Materials

While an organization’s Information Security Awareness Program should typically have its own specific and tailored “DNA,” reliable reference materials can help ensure that your organization incorporates industry best practices.

Some examples of reference materials include:

- National Institute of Standards and Technology (NIST) Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, www.nist.gov

- International Standards Organization (ISO) 27002:2013, Information Technology -- Security Techniques -- Code of Practice for Information Security Controls, www.iso.org

- International Standards Organization (ISO) 27001:2013, Information technology -- Security Techniques -- Information Security Management Systems, www.iso.orgCOBIT 5 Appendix F.2, Detailed Guidance: Services, Infrastructure and Applications Enabler, Security Awareness, www.isaca.org/cobit

Steps to Develop an Information Security Awareness Program

1. Evaluate Current State

The first step is to define the baseline by determining the current state of security awareness of the organization. Unless you know where you are along the route, you cannot align yourself to your goal. Organizations should analyze current “security awareness health” using different techniques to arrive at an all-inclusive snapshot. Some examples of these techniques include:

- Interview management, operational staff, support staff, and other organizational staff
- Review organizational culture
- Complete organizational surveys
- Review current awareness training materials and resources
- Complete social engineering assessments
- Analyze current metrics
- Review system and application inventory
- Analyze current industry trends
- Review industry regulations and standards
- Analyze prior security events and incidents

Once the analysis is complete, organizations should then identify and measure the gap between the current state of security awareness and the desired/target state.

2. Develop an Information Security Awareness Program

Four key components will define the quality of your Information Security Awareness Program:

- Who – Target audience
- What – Content
- How – Delivery method
- Why – Success criteria and metrics

The traditional "Pavlovian approach" to Information Security Awareness Training has often proven ineffective. For instance, a typical Phishing training would tell users not to click on links in e-mails and the post-training tests would involve sending test e-mails to users to see if they click on those links. Most likely, they will not click. The organization might assume that to be a success metric based on the employees' well-tuned Pavlovian responses.

Instead, the goal of Information Security Awareness should be to create "thinking employees." It is important to focus on making employees "street smart" when it comes to recognizing new tricks and techniques that hackers will employ from time to time. Think of it this way: You give someone a fish, and you feed them for a day; teach someone to fish and you feed them for a lifetime.

Organizations should also understand that employees need to find a certain level of engagement with the training material. The material needs to be unique, interesting, thought-provoking, and, if possible, nothing like anything they've seen before. This promotes employee "buy-in," which means the organization is halfway there.

Target Audience

- Create target audience segments by grouping training efforts by function, level, departments, and/or locations. Some examples of target audience segments include Executives, Information Technology, Sales and Marketing, Human Resources, Finance and Accounting, and Staff.
- Some training content will apply to all target audience segments.
- Some training content will need to be tailored based on the unique guiding factors per target audience segment (e.g. by level, risk level, function, etc.).

Content

- The training content should be innovative and engaging, tailored to skill level, include storytelling, contain a breadth of topics, include corporate and personal relevance, be customized, be focused on behavior and culture change, and include reinforcement through active campaigns.

- Below are some example topics based on PCI DSS and NIST best practices:
    - Individual accountability statements
    - Acceptable use policy
    - Password security
    - Email security
    - Smartphone security
    - Web security
    - Data access controls
    - Data backup security
    - Social engineering
    - Incident response
    - Physical security
    - Security on the move
    - Encryption
- Each topic should be designed for basic, intermediate, or advanced audiences depending on the target audience user group.
- Training content may be developed in-house, by a third party, or a combination of both. Many vendors offer Information Security Awareness Training. For example, **ERMProtect™** is a unique, innovative, and intuitive Information Security Awareness Training platform that includes a range of topics, formats, and functionality. A description of **ERMProtect™** is contained within Appendix A.

Delivery Method

- There are several delivery models (e.g. paper-based, cloud-based, instructor-led, online webinars and courses, etc.) and multiple delivery types (e.g. traditional lecture, lunches, town hall meetings, contests, games, interactive sessions, simulators, table top exercises, login messages, banners, etc.).
- Organizations should tailor the delivery models and types to the target audience groups based on organizational needs and training success factors.
    - Some examples of what you should look for in terms of training success factors include ease of use, whether training is motivating, whether it is challenging, whether it is fun, and whether it brings about positive reinforcement.
    - Some examples of training goals include user behavior change and return on investment.

Success Criteria

- Organizations must define success criteria and metrics upfront to be able to measure and communicate results.
- The specific metrics vary by organization type, size, industry, and goals.
- Some examples of success criteria include incident reporting, survey/assessment results, simulated tests, industry benchmarks, and return on investment.

3. Implement the Information Security Awareness Program

After the program is developed, the organization should implement the program. Implementation can be in stages (e.g. by target audience) or all at once. The organization should carefully plan the implementation.

- Define the implementation timeline
- Determine activities and communication based on target groups
- Create timelines for the different activities
- Develop a project implementation work plan
- Review, refine, and finalize the program
- Create a timeline for metrics review
- Create a timeline for revisions/adjustments (if needed)

Implementation best practices include an initial communication from top management expressing support for the project, followed by continual communications that identify short-term wins and improvements. As always, it is important that communications are tailored by target audience segment as no single communication will evoke action/responses from every segment within an organization.

4. Maintain the Information Security Awareness Program

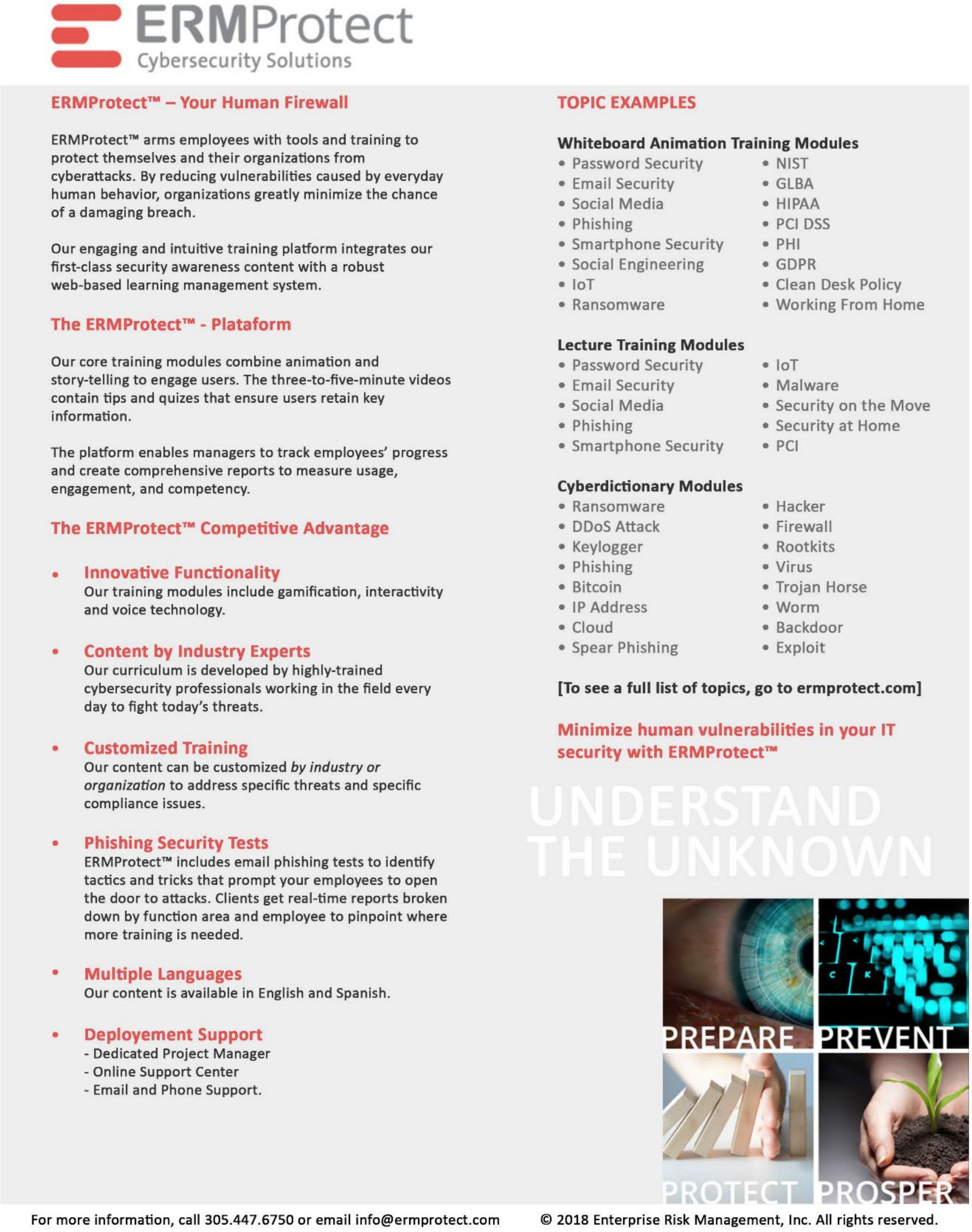
Maintaining the Information Security Awareness Program should be a joint effort by the Board of Directors, Senior Management, Chief Information Security Officer, Information Security Department, IT Department, Risk Management Department, Legal Department, Production and Deployment Department, and Human Resources. An organization should review and update the Information Security Awareness Program at least once a year or when there are significant changes in the organization’s IT infrastructure, threat landscape, risk composition, or regulatory responsibilities.

5. Measure and Track Performance Metrics

The organization should regularly measure, track, and communicate the results of Information Security Training efforts. Communicating the status of the Information Security Awareness Program ensures that stakeholders are aware of the organization’s security awareness “health” and the overall return on investment they are getting from the effort.

Appendix A

ERMProtect™ - Information Security Awareness Training Platform



ERMProtect
Cybersecurity Solutions

ERMProtect™ – Your Human Firewall

ERMProtect™ arms employees with tools and training to protect themselves and their organizations from cyberattacks. By reducing vulnerabilities caused by everyday human behavior, organizations greatly minimize the chance of a damaging breach.

Our engaging and intuitive training platform integrates our first-class security awareness content with a robust web-based learning management system.

The ERMProtect™ - Plataform

Our core training modules combine animation and story-telling to engage users. The three-to-five-minute videos contain tips and quizes that ensure users retain key information.

The platform enables managers to track employees' progress and create comprehensive reports to measure usage, engagement, and competency.

The ERMProtect™ Competitive Advantage

- **Innovative Functionality**
  Our training modules include gamification, interactivity and voice technology.
- **Content by Industry Experts**
  Our curriculum is developed by highly-trained cybersecurity professionals working in the field every day to fight today's threats.
- **Customized Training**
  Our content can be customized *by industry or organization* to address specific threats and specific compliance issues.
- **Phishing Security Tests**
  ERMProtect™ includes email phishing tests to identify tactics and tricks that prompt your employees to open the door to attacks. Clients get real-time reports broken down by function area and employee to pinpoint where more training is needed.
- **Multiple Languages**
  Our content is available in English and Spanish.
- **Deployement Support**
  - Dedicated Project Manager
  - Online Support Center
  - Email and Phone Support.

TOPIC EXAMPLES

Whiteboard Animation Training Modules

- Password Security
- Email Security
- Social Media
- Phishing
- Smartphone Security
- Social Engineering
- IoT
- Ransomware
- NIST
- GLBA
- HIPAA
- PCI DSS
- PHI
- GDPR
- Clean Desk Policy
- Working From Home

Lecture Training Modules

- Password Security
- Email Security
- Social Media
- Phishing
- Smartphone Security
- IoT
- Malware
- Security on the Move
- Security at Home
- PCI

Cyberdictionary Modules

- Ransomware
- DDoS Attack
- Keylogger
- Phishing
- Bitcoin
- IP Address
- Cloud
- Spear Phishing
- Hacker
- Firewall
- Rootkits
- Virus
- Trojan Horse
- Worm
- Backdoor
- Exploit

[To see a full list of topics, go to ermprotect.com]

Minimize human vulnerabilities in your IT security with ERMProtect™

For more information, call 305.447.6750 or email info@ermprotect.com

Appendix B

SAMPLE OF FREE SECURITY AWARENESS RESOURCES:

http://cias.utsa.edu/assets/free-awareness-resources.pdf

https://www.cybrary.it/

http://iase.disa.mil/eta/Pages/index.aspx

http://irtsectraining.nih.gov/publicUser.aspx

http://www.ussecurityawareness.org/highres/index.html

http://www.gideonrasmussen.com/

http://www.sans.org/security_awareness.php

http://ims.uthscsa.edu/information_security/information_education.aspx

http://www.csoonline.com/article/221057/Security_Awareness_Programs_Now_Hear_This_

https://free.thesecurityawarenesscompany.com/

http://csrc.nist.gov/organizations/fissea/2006-conference/Lindholm-FISSEA2006.pdf

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

https://infosecdojo.files.wordpress.com/2016/06/9-1-final-infosec-program-proposal.pdf

https://www.cisco.com/c/dam/en_us/about/security/cspo/docs/measuring_effective.pdf

https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

https://www.sans.edu/student-files/projects/ExecutionPlanPub.pdf

https://thesai.org/Downloads/Volume8No2/Paper_26-A_Framework_for_an_Effective_Information_Security_Awareness.pdf