Security Awareness and Training

SOLVING THE UNINTENTIONAL INSIDER THREAT

Michelle Ward, CEO and Founder
CYBER SAFE WORKFORCE LLC | PO BOX 4932 FORT WALTON BEACH, FL 32549

TABLE OF CONTENTS

INTRODUCTION

No organization wants to face a data breach. Lawsuits, penalties, and fines are just the beginning. Breaches also have a negative, lasting impact on the organization's reputation. Security awareness and training, when done properly, helps reduce risk to an organization's data and information systems, thereby reducing interruptions to business operations and limiting the chance of a data breach.

BACKGROUND

As cyber security concerns grow, the unintentional insider threat is among the top identified risks. Approved users, often employees, pose a major threat to a company's security.

Unintentional Insider Threat

Information Technology (IT) managers and staff know that EMPLOYEES MAKE UP THE LARGEST ATTACK SURFACE in their network. Employees spend their days performing duties such as reading e-mail, visiting websites, and answering phones. With each action comes risk, as these activities have been consistently exploited by cyber criminals.

E-mail is a vector for phishing[1] and business e-mail compromise (BEC)[2].

- Business e-mail compromise (BEC) was responsible for the loss of $750 million from U.S. companies from October 2013 to August 2015.[3]
- According to the Verizon 2015 Data Breach Investigations Report, phishing e-mails are opened by 23% of recipients with 11% clicking on attachments.

[1] Phishing e-mails are scams to get users to infect their machines or reveal sensitive information such as login credentials.
[2] Business e-mail compromise is the act of obtaining access to an executive's e-mail in order to send legitimate-looking e-mails often used to request financial wire transfers.
[3] Retrieved 09 March 2016 from http://krebsonsecurity.com/2015/08/fbi-1-2b-lost-to-business-email-scams/

Websites can allow for drive-by infections and phishing.

- Hacked websites can trick users into downloading malicious software or into providing login credentials or other personal information.
- According to the Webroot® 2016 Threat Brief, suspicious URLs do not always appear on sites within a dubious category. The second highest category identified as hosting suspicious URLs in 2015 was "business and economy" websites. Top impersonated companies included Google, PayPal, Dropbox, Yahoo, Bank of America, Apple, and Facebook.

The phone is a means for a social engineering technique known as vishing (voice phishing).

- Vishing can be used to solicit enough information to execute additional attacks, including physical access.
- According to Social-Engineer.org, 67% of people asked will provide social security numbers, birthdates, or employee ID numbers.[4]

Additional statistics:

- Ninety percent of security incidents categorized in the Verizon 2015 Data Breach Investigations Report featured a human element.
- According to the Verizon 2016 Data Breach Digest, 80% of data breaches are related to poor password hygiene.

How might an employee's actions lead to a shutdown of normal business operations?

In February 2016, the Hollywood Presbyterian Medical Center in Los Angeles paid $17,000 to cyber criminals to restore their systems after becoming infected with ransomware. Ransomware, which is spread through hacked websites or malicious e-mail attachments, locks files on the network with unbreakable encryption algorithms. The hospital spent almost a week without the use of their computer network and had to revert to using paper forms.[5]

[4] Retrieved 09 March 2016 from http://www.social-engineer.org/social-engineering/social-engineering-infographic/

[5] Retrieved on 10 March 2016 from http://arstechnica.com/security/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/

Who Maintains Responsibility?

Envision a doctor's office that does not train employees with respect to disclosing patient medical information. Imagine if a nurse simply gave out test results to anyone who called in claiming to know the patient. This seems unimaginable, as all patients sign a medical information release form specifying with whom their records may be discussed. The average medical professional may not realize that sending Protected Health Information (PHI) through e-mail without encryption means that third-parties may see that information.

The typical user simply wants to get their work done and may see computer security as a hindrance to their tasks, too technical to understand, or someone else's job (i.e. Information Technology's). However, there is no technological solution that will prevent 100% of cyberattacks.

SECURITY MANAGERS CANNOT STAND BEHIND THE SHOULDER OF EVERY USER DURING EVERY E-MAIL, WEBSITE, OR PHONE INTERACTION.

Can an employee, who has received inadequate or no training, be blamed for inadvertently allowing cyber criminals into the network?

SOLUTION

SECURITY AWARENESS AND TRAINING FOR ALL USERS (EMPLOYEE/PARTNER/CONTRACT) IS THE SOLUTION TO THE INADVERTENT INSIDER THREAT.

Security awareness and training is required for compliance with a number of laws and regulations and is a security control within information security management frameworks.

Security Awareness in Laws and Regulations

Some laws and regulations that specify the need for security awareness and training include:

- Healthcare: Health Insurance Portability & Accountability Act (HIPAA) §164.308.(a).(5).(i)
- Payment Industry: Payment Card Industry Data Security Standard (PCI DSS) §12.6
- Public Companies: Sarbanes-Oxley (SOX) §404(a).(a).(1)
- Federal Agencies: Federal Information Security Management Act (FISMA) §3544.(b).(4).(A),(B)

In addition, states may also have security awareness and training as part of their communications or privacy laws. For example, the State of Florida's Information Security Technology Act FL Stat §282.318 (2014) indicates that all IT security plans should:

"Provide information technology security awareness training to all state agency employees concerning information technology security risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks."

User Training Requirements Within Information Security Management Frameworks

Information security frameworks that include security awareness and training for all employees (and partner users):

- NIST Cybersecurity Framework (CSF) PR.AT
- NIST Risk Management Framework (RMF) through NIST SP 800-53 Rev. 4 AT-2
- ISACA Control Objectives for Information and Related Technology (COBIT) 5 APO07.03, BAI05.07
- ISO/IEC 27001:2013 A.7.2.2

Security awareness and training is most often identified as an avenue to *protect* information, as educating users leads to a reduction in security incidents.

Security Awareness and Training Program Evaluation

Using the NIST Cybersecurity Framework as a guide, organizations can evaluate which tier best matches their current security awareness and training program.

Tier 1	Partial	Security awareness and training is ad hoc or reactive. User education may only take place after an incident (e.g. mass e-mail all users after one has been infected with ransomware). There is limited awareness of risk at the organizational level, and there may be a lack of support for an awareness and training program (i.e. computer security is seen as an IT function only).
Tier 2	Risk Informed	Awareness may be delivered through periodic newsletters or posted to an intranet portal without tracking user participation. No formal curriculum is defined. Support for a program has been approved, but there is no policy adopted by the organization.
Tier 3	Repeatable	Awareness and training is mandatory for everyone and is tracked. Training may be updated based on changes in technology, changes to security controls, and new threats. A formal policy is in place which includes periodic reviews and updates.
Tier 4	Adaptive	Awareness and training is mandatory for everyone and is tracked and measured. Training is updated based on feedback, changes in technology, changes to security controls, and new threats. A formal policy is in place which includes periodic reviews and updates.

Table 1 Security Awareness and Training Evaluation

Security Awareness and Training Program Structure

A successful security awareness and training program can be modeled as a lifecycle. Using this model, an organization can maintain a Cybersecurity Framework Tier 3 or 4 security awareness and training program.

Each activity in the lifecycle is discussed in the following sections.

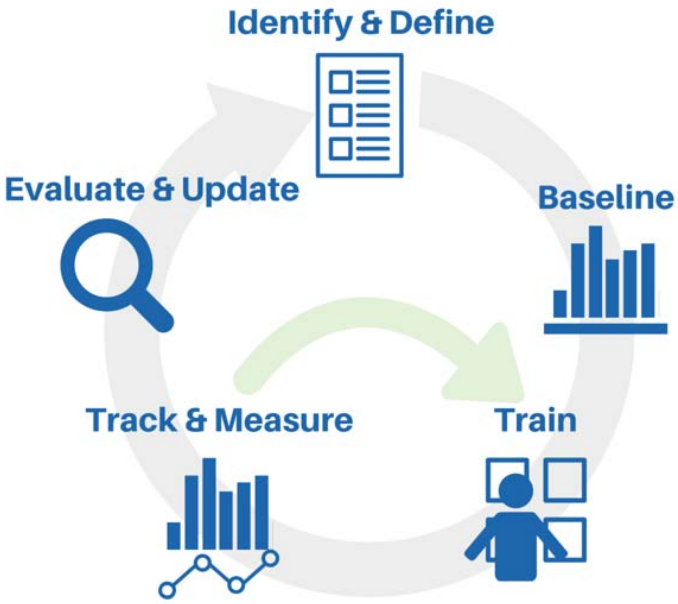

Figure 1 Security and Awareness Training Lifecycle

IDENTIFY AND DEFINE

In this step, define the security and awareness training program by creating a policy that meets all the criteria of the NIST SP 800-53 Rev. 4 AT-1 security control. Create a training plan that defines topics to be covered, how it will be delivered, and criteria by which it will be measured.

Topics will be influenced by applicable laws and regulations, security controls and procedures, threat information, as well as frequent user issues identified by the technology help desk.

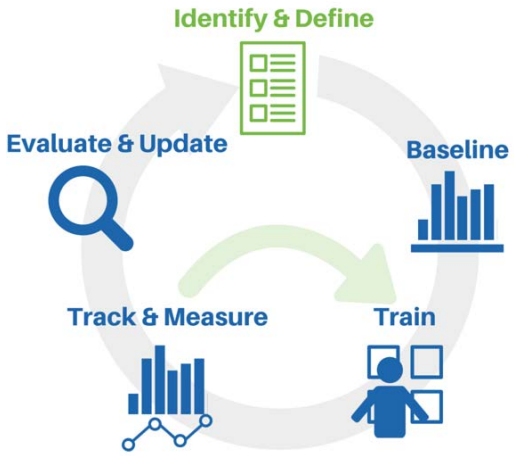

Figure 2 Identify & Define

Activities	*Artifacts*
Define the scope, roles and responsibilities, compliance, update interval, etc. (NIST SP 800-53 Rev 4 AT-1)	Security and Awareness Training Policy
Define the curriculum and learning objectives, the organization's goals, how goal progress will be measured, delivery methods, and time frames.	Security and Awareness Training Plan

BASELINE

To create a baseline, gather an initial set of data prior to implementing training. This data will be used to later measure the effectiveness of security awareness and training.

EXAMPLE

If a goal is to "reduce incidents related to account credential disclosure by 75%", obtain the number of account credential disclosures for the past X days.

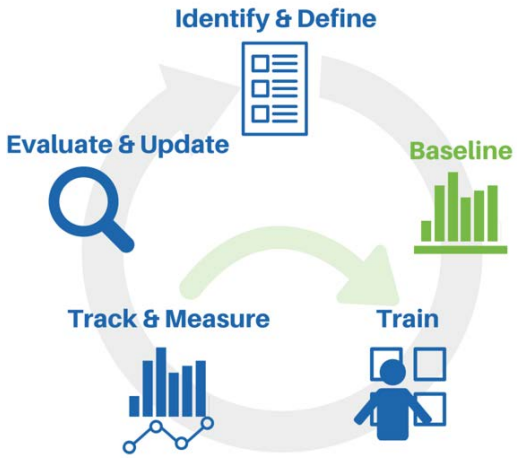

Figure 3 Baseline

Activities	*Artifacts*
Gather metrics for goals defined in the Security Awareness Training Plan	Security and Awareness Training Report

TRAIN

In the training step, deliver the guidance and information. Training may be executed online, during employee on-boarding, with on-site classes, etc.

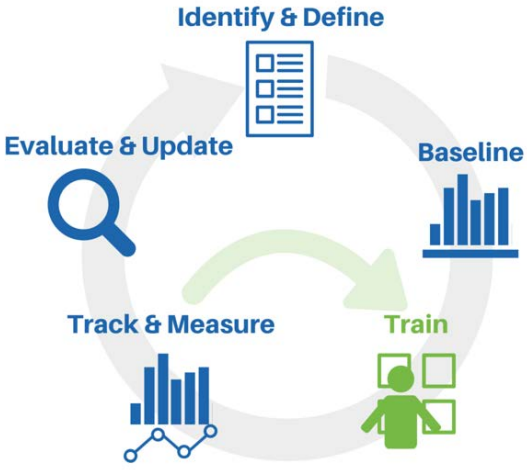

Figure 4 Train

Activities	*Artifacts*
Announce/Introduce training	Notifications
Conduct training	Training participation log, Training completion report, user scores

TRACK AND MEASURE

To track and measure progress, audit participation in the training program and gather metrics for goals. If participation needs remediation, go back to the Train step.

Because training can take place incrementally throughout the year, there may be several cycles of Train and Track and Measure.

Optional activities include: surveying users for feedback and conducting penetration tests.

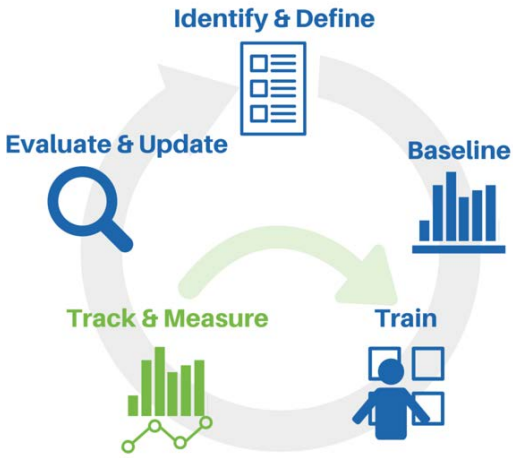

Figure 5 Track & Measure

Activities	*Artifacts*
Audit participation	Security and Awareness Training Progress Report
Gather metrics for goals defined in the Security Awareness Training Plan	Security and Awareness Training Report
Survey users	Survey Results
Conduct social engineering penetration test	Penetration Test Report

EVALUATE AND UPDATE

In the final step in the lifecycle, review data gathered during the Track and Measure phase, new threat information, information security policy changes, and new technical controls or systems. Use this information to update the Security Awareness and Training Policy or Plan.

This step ensures that the Security and Awareness Training program will continue to evolve as the environment and threat landscape evolves.

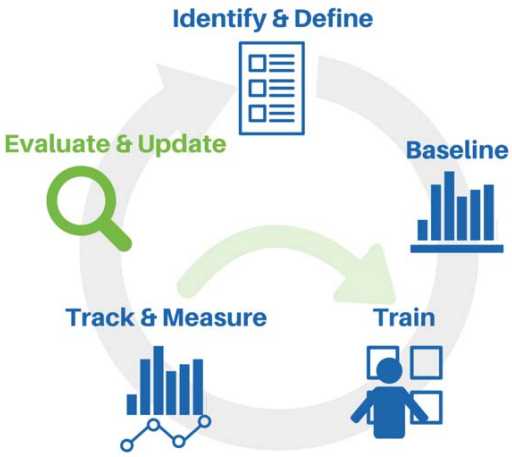

Figure 6 Evaluate & Update

Activities	*Artifacts*
Review Security Awareness and Training Report, other artifacts gathered throughout the life cycle, threat information, information security policy changes, and new technology introduced.	
Identify changes to the current security awareness and training program.	Updated Security Awareness and Training Policy and Security Awareness and Training Plan

HOW CYBER SAFE WORKFORCE LLC CAN HELP

Cyber Safe Workforce LLC partners with your organization to close the knowledge gap by providing the security expertise, framework, materials, and hands-on guidance needed to implement an effective security awareness and training program.

Our goal is to improve the efficacy of your awareness and training program, based upon your overall cyber security goals.

Cyber Safe Workforce LLC can help your organization:

- Establish a Security Awareness and Training Policy that meets the NIST 800-53 Rev. 4 AT-1 control.
- Create a Security Awareness and Training Plan that incorporates all aspects of the Security Awareness and Training Lifecycle.
- Identify key security awareness topics.
- Customize security awareness and training curriculum for your environment.

CONCLUSION

Information Technology security managers know that employees are the largest attack surface in their network, with daily tasks being successful vectors of compromise. The average user is focused on doing their job and often will not make the connection between their actions and potential security incidents. The answer is to educate employees through quality security awareness and training. In many industries, an awareness and training program is required for compliance with a number of laws and regulations and is a component of information security management frameworks. Cyber Safe Workforce LLC can help meet these requirements and protect your organization's network by providing the framework, materials, and guidance to implement a successful security awareness and training program.

WWW.CYBERSAFEWORKFORCE.COM

1-877-829-4229