Optimum Security Cognizance Through People, Process and Behavior Transformation

The importance of cybersecurity in enterprise ecosystems is constantly being communicated to the workforce to create awareness, which helps enterprises reduce their attack surfaces. Public news of data leaks can harm an enterprise's market reputation. Particularly when staff members have easy access to sensitive information such as client data, personnel data, trade secrets and user credentials, the threat of intentional or unintentional data leakage is high. Therefore, it is critical to manage the potential security threats posed by staff. To address these insider threats and improve security cognizance, information security leaders must prioritize well-defined transformation efforts driven by people, process and behavior perspectives based on international good practices, guidelines on training methodologies[1, 2, 3] and automated solutions.[4]

People Transformation

To instill and improve security cognizance in an enterprise, a detailed security competency framework should be developed and implemented. This helps ensure that all staff members and third parties have the appropriate security training and awareness to proactively identify and prevent security breaches. Staff should be divided into target groups and mapped to various security competencies, which should then be mapped to relevant security training at the next level. This three-level mapping helps ensure that the appropriate groups of staff receive the appropriate security training and acquire the appropriate security competencies. Lack of appropriate competencies and unavailability of relevant training are critical factors leading to insider data leaks.

Figure 1 lists critical security competencies and the groups of staff to which they pertain.

Important information security training topics based on a well-defined competency framework include:

- General information security awareness
- Information security program
- Data leakage detection and prevention
- User access management
- Secured software development
- Information security incident management
- Human resources security
- Physical and environmental security
- Third-party security

VIMAL MANI | CISA, CISM, SIX SIGMA BLACK BELT

Is the head of the information security department of Bank of Sharjah. He is responsible for the bank's end-to-end cybersecurity program, coordinating cybersecurity efforts within the banking operations spread across the Middle East. Mani is also responsible for coordinating bankwide cybersecurity strategy and standards, leading periodic security risk assessment efforts, incident investigations and resolution, and coordinating the bank's security awareness and training programs. He is an active member of the ISACA® Dubai (United Arab Emirates) Chapter. He can be reached at vimal.consultant@gmail.com.

FIGURE 1

Critical Security Competencies by Staff Groups

Security Competencies Identified	General Staff	System and Network Administrators	Software Development	IT Operations	Human Resources (HR) Operations	Physical Security	Third Parties	Information Security	Executive Management
Social engineering	Y	Y	Y	Y	Y	Y	Y	Y	Y
Secure software development and application security	N	N	Y	Y	N	N	N	Y	N
IT infrastructure security	N	Y	N	N	N	N	N	Y	N
Network security	N	Y	N	N	N	N	N	Y	N
Data loss prevention	Y	Y	Y	Y	Y	Y	Y	Y	Y
Vulnerability management	N	Y	Y	Y	N	N	N	Y	N
Third-party security	Y	Y	Y	Y	Y	Y	Y	Y	N
Information security incident management	Y	Y	Y	Y	Y	Y	Y	Y	Y
Physical and environmental security management	Y	Y	Y	Y	Y	Y	Y	Y	Y

- Infrastructure security
- Vulnerability analysis
- Penetration testing
- Information systems continuity planning

Process Transformation

To improve the security cognizance level in an enterprise, the end-to-end security awareness process needs to be reengineered and redesigned by considering critical activities such as training needs analysis, training delivery schedule, content development and delivery methods.

Training Needs Analysis

To identify the information security training needs of various target groups, an enterprise should:

- Identify the target audiences for the proposed training.
- Identify the information security competencies required for the target groups and develop a competency framework.
- Conduct a gap assessment based on the competency framework, identifying the information security skills required vs. the skills available within the target groups.
- Identify baseline training needs (general and specific training).

Training Delivery Schedule and Participation

Based on the training needs analysis, a suitable weekly training schedule should be prepared.

Appropriate communication should be established with all the identified audiences, requesting that they confirm their participation in the scheduled training sessions. Continual follow-up should be performed to ensure effective participation. Attendance at mandatory training can be waived only with the approval of appropriate levels of management, supported by valid justification.

Development of Training Content

When designing information security awareness courses, enterprises should consider learning objectives, learning activities and assessments that staff can pursue and complete in a timely manner.

The training content should be customized by considering the various users and their learning preferences, and the content should include appropriate examples that relate to the context of the enterprise and its information-sensitive ecosystem. The training delivery and content should be aligned with the participants' defined roles and responsibilities.

It is important to note that the creation of customized training content is a complex and time-consuming activity. One option is to hire subject matter experts to

coordinate with the various target groups of staff to understand their training needs and create exclusive and customized training content, but this is a significant expense, especially for smaller enterprises.

On an ongoing basis, new training can be scheduled based on key triggers identified. Moreover, training and awareness material can be updated based on feedback from audiences through training effectiveness evaluation and critical organizational changes. Methods for creating awareness are illustrated in **figure 2**.

Training Delivery Mechanisms

Internal and external resources can be leveraged to create and deliver training.

Content for general information security training should be prepared internally and rolled out through the enterprise's internal elearning platform. Focused classroom sessions can be planned for special training as needed. Training sessions should be formally announced in advance to ensure that staff are available to participate.

Carefully selected vendors can deliver customized information security training on various topics, such as mobile security and online banking security. These vendors design and deliver training based on the needs of the enterprise.

Evaluation of Training

If planned and delivered training programs are not achieving the expected results in an organization, conducting a thorough training evaluation will help the organization make effective changes for future programs. Based on such an evaluation (supported with return on investment [ROI] analysis), organizations may modify or discontinue a training program planned for the future.

FIGURE 2
Creating Awareness

Awareness Creation Method	Description and Implementation
Posters, flyers and newsletters	• Posters and flyers can be used to create information security awareness on individual topics. They should be displayed in areas where people gather, such as cafeterias and meeting rooms, as well as in elevators, lobbies and restrooms. They can be used to highlight time-sensitive issues and remind people of specific actions required to improve the enterprise's security posture. Posters should be changed periodically. • Periodic newsletters (e.g., monthly or quarterly) can be used to create widespread awareness. An advantage of newsletters is that they can convey multiple messages at the same time, whereas a poster conveys only one message. To be effective, newsletters require a proper distribution mechanism.
Blogs, screen savers, pre-login messages, emails and intranets	• Blogs can be used to educate staff on organizational policies and internal affairs. • Screen savers and pre-login messages bring awareness directly to employees' desktops and their daily work environment. The advantage of screen savers is that everyone sees them multiple times a day. Screen savers need to be changed often to introduce new information security topics. • Emails and an intranet can be used to post information security tips and weekly or monthly columns about the enterprise's security initiatives. Using emails and an intranet can reach a wide audience in one step.
Recorded videos	Information security awareness videos play an important role in the awareness program. There is no need for a classroom trainer or an elearning course. Video is an effective medium that can provide visual and audio education. Learners can study independently, learn at their own pace and get tailored content based on what they need to know. Moreover, videos can be watched and rewatched as needed, making them a flexible and effective training choice. However, videos can be expensive.
Events conducted by partners	Exclusive information security awareness events conducted by partners such as a community emergency response team (CERT) can create awareness on various topics for various levels of staff.

Several steps are required to evaluate the effectiveness of information security training and awareness programs:

- Give assessment tests immediately after training delivery to measure the audience's understanding of the content.
- Distribute a well-defined survey questionnaire to the audience's reporting managers after the completion of training to determine its effectiveness.
- Send follow-up questionnaires to staff members who attended classroom training in the previous six months to determine how well they retained the knowledge imparted during training.
- Monitor the number of information security compliance issues and breaches. Is this number decreasing or increasing? Why? Although an increase in the number of compliance issues and breaches may be a sign that the training has some weaknesses, an increase in the reporting of compliance issues and breaches may indicate greater awareness, which is a sign of training effectiveness and success.
- Conduct spot checks of personnel behavior. For instance, walk through work areas and note whether users are logged in while workstations are unattended.
- Record user IDs and completion status for web-based online training. Send a targeted questionnaire to those who have completed the online training.
- Have training participants fill out evaluation forms at course completion.
- Conduct an after-hours walkthrough to document all information security and privacy risk factors and violations prior to training. Then, approximately one to three weeks after training, conduct another walkthrough to document whether security and privacy risk factors have decreased, indicating effectiveness of the training or awareness activity.

Maintenance of Training Records and Management Review

Training-related records such as the plan, schedule, attendance report, and evaluation forms should be maintained for future reference. Archiving and maintaining training-related records serves as evidence of the effectiveness of the training programs conducted in the organization. They will also serve as effective inputs toward corrective and preventive actions, management reviews, internal and external audit and assurance activities held in the organization, future employee skills development and overall management of the organization. It is recommended that these training records be stored for at least five years, but times may differ based on local and international regulations.

All programs planned and delivered should be reviewed by senior management for their objectives, adequacy and budgetary support required on a periodic basis. These programs need to be presented to the leadership team after review and approval by the security steering committee. The internal audit and compliance team should also audit these programs as part of its periodic reviews.

Enterprises can simulate well-designed social engineering attacks—such as phishing, vishing and smishing and in-person social engineering attacks—to observe how staff members react to them.

Behavior Transformation

Human error and negligence can lead to cyberattacks; therefore, assessing human behaviors is critical for understanding potential cyberrisk.[5] Enterprises should consider techniques such as social engineering simulations, spot audits, incentives and identification of security champions to assess and fine-tune staff behavior related to the handling of the various information and cybersecurity incidents they may encounter in their day-to-day jobs.

Social Engineering Simulations

At periodic intervals, enterprises can simulate well-designed social engineering attacks—such as phishing, vishing and smishing and in-person social engineering attacks—to observe how staff members react to them. Staff behavior when handling simulated security incidents should be carefully analyzed and appropriate corrective measures should be taken.

Spot Audits and Incentives

Enterprises can conduct spot audits of desks to check how securely employees maintain their workspaces and adhere to the enterprise's clear screen and clear desk policy. This policy is intended to ensure that sensitive information and various information assets available at personal and public workplaces are protected even when they are not in use or when someone leaves their workstation for a short time.[6] Those staff members who showcase good compliance can be awarded with incentives on the spot. This motivates employees to ensure the security of their workspaces and protect the information assets of the enterprise.

Enterprises should consider revisiting the people, process and behavioral aspects of their information security policies and continually reengineer them to achieve the optimum level of security cognizance.

Security Champions

To improve staff behavior in the handling of security incidents, enterprises can select security champions from every business unit, every business function or every floor. These identified personnel are then provided with focused security awareness training and educated on their responsibilities as security champions. On a periodic basis, discussions should be held with these security champions, and their good efforts should be recognized with incentives to improve their morale and behavior.

Conclusion

The objective of an information security awareness program is not for everyone to become security professionals. It is to educate staff on how to be security-aware and to identify and report potential security threats. But for many contemporary enterprises, this requires a significant change in culture. For security leaders, it is critical to demonstrate that the information security awareness program has a positive impact on the overall security culture of the enterprise.

Improving security awareness is not a onetime exercise; security training should be rolled out every four to six months. This allows leadership to make staff aware of the threat landscape and the security posture of the enterprise at that point in time. Training sessions should be short (30 to 45 minutes) and focused.

Educating staff on internal security policies is an excellent way to communicate an enterprise's information security culture and acceptable information security behavior by staff. But these policies should be mature and in line with global security standards before training is provided. Best practices[7, 8, 9] related to information security training and awareness should be analyzed, and those that are most suitable to the organizational culture should be implemented. Automated solutions are available in the market that can make customized program rollout easier for security leaders.[10] Enterprises should consider revisiting the people, process and behavioral aspects of their information security policies and continually reengineer them to achieve the optimum level of security cognizance.

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Endnotes

1 European Union Agency for Network and Information Security (ENISA), *Good Practice Guide on Training Methodologies*, Greece, 12 November 2014, *https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies*

2 European Union Agency for Network and Information Security (ENISA), *Information Security Awareness in Financial Organisations*, Greece, November 2008, *https://www.enisa.europa.eu/publications/archive/is-in-financial-organisations/at_download/fullReport*

3 PCI Security Standards Council, *Information Supplement: Best Practices for Implementing a Security Awareness Program*, USA, October 2014, *https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf*

4 Andriotis, N.; "Training Automation: Seven Reasons Your Employees (And Bottom Line) Need It," eLearning Industry, 29 July 2019, *https://elearningindustry.com/how-automated-training-benefits-employees-business*

5 Burch, G. F.; J. H. Batchelor; R. Reid; T. Fezzey; C. Kelley; "Drawing Connections Between Security and Employee Personalities," *@ISACA*, 22 December 2021, *https://www.isaca.org/resources/news-and-trends/newsletters/*

atisaca/2021/volume-43/drawing-connections-between-security-and-employee-personalities

6 Leal, R.; "Clear Desk and Clear Screen Policy and What it Means for ISO 27001," 27001 Academy, 14 March 2016, *https://advisera.com/27001academy/blog/2016/03/14/clear-desk-and-clear-screen-policy-what-does-iso-27001-require/#:~:text=9%20%E2%80%93%20clear%20desk%20and%20clear%20screen%20policy%20requires%20pretty%20low,and%20similar%20only%20when%20authorized*

7 European Union Agency for Network and Information Security (ENISA), *Good Practice Guide on Training Methodologies*, Greece, 12 November 2014, *https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies*

8 European Union Agency for Network and Information Security (ENISA), *Information Security Awareness in Financial Organisations*, Greece, November 2008, *https://www.enisa.europa.eu/publications/archive/is-in-financial-organisations/at_download/fullReport*

9 PCI Security Standards Council, *Information Supplement: Best Practices for Implementing a Security Awareness Program*, USA, October 2014, *https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf*

10 KnowBe4, "Get Your Customised Automated Security Awareness Program, ASAP," *https://www.knowbe4.com/me-asap-ga?utm_term=information%20security%20awareness&utm_campaign=Google_NonBrand_Security_Awareness_Training_Search_ME&utm_source=google&utm_medium=ppc*