Considerations for Developing Cybersecurity Awareness Training

Human error has always been a leading cause of cybersecurity breaches. According to Verizon's *2022 Data Breach Investigations Report*, 82 percent of data breaches involve the human element.[1] Whether the breach results from stolen credentials, phishing, misuse or a simple error, people play the largest role in these incidents. Therefore, it is important to implement effective cybersecurity awareness training to help employees understand proper cyberhygiene, recognize the security risk factors associated with their actions and identify cybersecurity incidents they may encounter in their work.

Cybersecurity awareness training must be tailored to the access rights of employees.

Regular, ongoing cybersecurity awareness training is important, and the best time to start is during the new employee onboarding process. This sets the correct expectations in terms of what to do and what not to do before a new employee has access to the enterprise's information assets or data.

There are many considerations when developing a comprehensive cybersecurity awareness training program for employees. Ideally, program developers should ask the following questions:

- What are the employee's access rights?
- What constraints and practices must an employee agree to (e.g., acceptable use policy [AUP]) before gaining access to the enterprise's information assets or data?
- Of what legislative, regulatory and contractual security obligations should an employee be aware?
- What are the potential threats faced by the enterprise in case of a breach?
- What is the appropriate response in the event of a cybersecurity incident?
- How will the effectiveness of cybersecurity awareness training be measured?
- How frequently should cybersecurity awareness training be conducted?
- What is the best option to deliver cybersecurity awareness training?

Access Rights

Depending on employees' roles and responsibilities, different access rights are required. For example, system administrators need privileged accounts to carry out their job duties, whereas system users need only nonprivileged accounts to access the system. Obviously, compromise of an employee with a privileged account has a bigger impact on the enterprise's information assets or data than compromise of an employee with a nonprivileged account. Similarly, operations managers require

TAN SOON CHEW | CISA, CRISC, CISM, CCSP, CISSP, PMP

Is an information security manager at Sita Information Networking Computing Pte Ltd., and an associate lecturer at the School of Engineering and Technology at PSB Academy (Singapore). He can be reached at soonchew.tan@psba.edu.sg.

physical access to the data center and the enterprise's physical assets to carry out their job duties, but they do not need logical access to the system. Therefore, operations managers do not require training on how to prevent cyberincidents related to logical access. Cybersecurity awareness training must be tailored to the access rights of employees.

AUPs

An AUP establishes an agreement between users and the enterprise and defines for all parties the ranges of use that are approved before access to a network or the Internet is granted.[2] Some enterprises may require employees to sign AUPs as part of the employment contract. Hence, it is important to emphasize the rules included in the AUP during cybersecurity awareness training. Other policies, standards and guidelines may be covered if they are relevant (e.g., password policy, clean desk policy, removable media policy).

It is important to emphasize the rules included in the AUP during cybersecurity awareness training.

Legislative, Regulatory and Contractual Security Obligations

Legislation is a directive imposed by a government or governing body on an industry, a section of a community or a country. An example is Singapore's Computer Misuse Act 1993.[3]

A regulation is a means of monitoring and enforcing legislation through specific rules developed by regulatory authorities. It can take various forms, such as an industry-specific regulation or one that is much broader in scope. One example is the EU General Data Protection Regulation (GDPR).[4]

A contractual security obligation is an agreement between two or more entities that has specific terms. It involves a binding agreement to perform a task or provide a service in return for consideration.

Including these obligations in cybersecurity awareness training reinforces their importance.

Cyberincident Response

Understanding threats related to human factors is crucial for any organization. Threats can include:

- Security threats involving physical access and device theft
- Social engineering (e.g., phishing, spear phishing)
- Malware (e.g., viruses, worms, Trojan horses, ransomware, spyware)
- Mobile device and online scams
- Social media threats

For any type of threat, employees must be trained to respond correctly once it has morphed into an attack. Employees must know when to report suspicious or confirmed cybersecurity incidents, whom to report the incident to and what communication channels are available for such reporting.

Effectiveness Measurement

The effectiveness of cybersecurity awareness training can be measured through:

- **Quizzes**—To validate employees' knowledge after training
- **Surveys**—To gather feedback from employees to improve existing training and create better training topics or materials for future employees
- **Number of reported cybersecurity incidents**—To assess employees' cybersecurity vigilance

Frequency of Training

It is recommended that enterprises hold cybersecurity awareness training every four to six months. At four months after initial training, employees are still able to spot phishing emails, but after six months, they start to forget what they have learned.[5]

Delivery of Training

Enterprises may consider using classroom-based training (physical, virtual or a mixture of both) or a learning management system (LMS) to automate the delivery and tracking of cybersecurity awareness training. There are many online LMS providers, such as Absorb LMS and SAP Litmos, and they provide useful tools for creating online courses, quizzes and surveys. After online courses are created, an enterprise can use the LMS to organize and distribute

ENJOYING THIS ARTICLE?

- Read *State of Cybersecurity 2022. www.isaca.org/go/state-of-cybersecurity-2022*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

online courses to its employees as needed. The LMS can also be used to monitor training progress, view analytics and allow employees to provide feedback in order for the enterprise to recalibrate its learning program for maximum impact.

Although online learning provides more flexibility to the trainees' schedules, classroom learning usually provides more interaction and engagement between the trainer and trainees. Depending on the nature or size of the enterprise, ease of delivery and cost are also key considerations for the type of delivery method used.

Conclusion

Conducting cybersecurity awareness training for new employees is only part of the equation. A comprehensive cybersecurity awareness program should be established and implemented to educate every person (including external vendors and their personnel) who uses, operates and manages the enterprise's assets or data. The purposes of the cybersecurity awareness program should be clearly defined, and the program's effectiveness should be measured at regular intervals (e.g., annually). The cybersecurity awareness program should also be reviewed at regular intervals (e.g., annually) to ensure that it remains current and relevant in the dynamic landscape of cybersecurity.

In the end, the aim is to positively shape individual behavior and enhance the security culture of the enterprise by reducing or minimizing the threat of cyberattacks related to the human element.

Endnotes

1 Verizon, *2022 Data Breach Investigations Report*, USA, 2022, *https://www.verizon.com/business/resources/reports/dbir/*

2 ISACA®, Glossary, *https://www.isaca.org/resources/glossary*

3 Singapore Statutes Online, Computer Misuse Act 1993, Singapore, *https://sso.agc.gov.sg/Act/CMA1993*

4 European Commission, " Data Protection—Rules for the Protection of Personal Data Inside and Outside the EU," *https://commission.europa.eu/law/law-topic/data-protection_en*

5 Reinheimer, B. *et al.*; "An Investigation of Phishing Awareness and Education Over Time: When and How to Best Remind Users," USENIX, 16th Symposium on Usable Privacy and Security, 2020, *https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf*