Cybersecurity Awareness Training
Questions Board Members Should Ask

Below are some questions you may ask management to ensure that the institution's cybersecurity awareness training program is sufficient to develop and maintain appropriate employee knowledge of ongoing and emerging threats against the institution.

1. ***How frequently does the institution conduct formal cybersecurity awareness training for all employees, including senior management and executives?***

   WHY THIS IS IMPORTANT: While annual training programs may be suitable for some institutions, there is growing evidence that more frequent cyber awareness training can be more effective. Organizations such as ISACA recommend training every four to six months to ensure that individuals more effectively retain the ability to apply what they have learned.[1] Institutions are encouraged to holistically examine the scope and track record of their cybersecurity training programs to determine the most appropriate frequency for delivery of employee awareness training. Training program requirements and tracking should extend to all individuals who are granted access to company data or systems, regardless of their position in the institution's hierarchy. This would also include any board members with institution email addresses or access to institution networks or systems.

2. ***Is there a program to track employee completion of assigned cybersecurity awareness training?***

   WHY THIS IS IMPORTANT: The institution should also implement a dynamic program to track employee compliance with training requirements. Management should frequently compare completed training assignment records and required due dates, and a process for follow-up, including escalation procedures for noncompliance, should be in place to ensure the completeness of training efforts for all employees.

3. ***Does the institution conduct phishing training to expose employees to simulate real-world threats?***

   WHY THIS IS IMPORTANT: While not a substitute for regular, full-scope cybersecurity training, periodically exposing all employees to random, simulated phishing emails more closely mimics what they see in daily real-world interactions and helps to both train and measure their ability to spot phony email messages, malicious attachments, and harmful links. This is particularly important given the growing sophistication and effectiveness of phishing techniques, such as AI-enhanced phishing, used by modern threat actors. Phishing exercises also provide trackable real-time metrics of employee awareness to institution management, which can guide future training efforts and help to identify areas where immediate refresher emphasis might be needed.[2]

4. ***Does the institution's training curriculum address:***

   a. ***Existing and emerging threats to the institution***

   b. ***Incident identification and reporting mechanisms***

[1] Chew, Tan Soon (ISACA). "Considerations for Developing Cybersecurity Awareness Training", March 1, 2023.
[2] Lewis, Jon (Cira). "How to Measure a Phishing Test Program", January 6, 2024.

c. ***Acceptable use policy training and employee acknowledgement***

WHY THIS IS IMPORTANT: Employees should be aware of the general threat landscape and the general nature of threat actor tactics, indicators and red flags, etc. While many training programs today address existing threats such as ransomware, phishing, insider threats, and social engineering, the recent emergence of artificial intelligence and the use of deep fakes by cyber threat actors, it is now most practical to consider these and other emerging areas when planning the training curriculum.

If an employee observes suspicious activity or inadvertently engages with a malicious email, file, or link, they should be keenly aware of the appropriate procedures for reporting such encounters to management or IT security teams. Moreover, they should feel no hesitation or fear of reprisal in reporting such encounters, regardless of whether they are suspected or actual incidents.

Formal training should include curricula addressing the expectations specific to the institution's acceptable use policy. A written attestation should ideally be obtained annually for every employee interacting with company systems (including senior and executive management) acknowledging that the policy has been read and its requirements are understood. [3]

5. ***Does the institution regularly expose employees to meaningful threat information, as appropriate, between formal training cycles?***

WHY THIS IS IMPORTANT: Due to the dynamic nature of the cyber threat environment, it is often necessary to provide employees with timely, meaningful information concerning emerging risks in between established training cycles. This can be accomplished through the regular delivery of threat information via awareness emails from IT security personnel or during branch or department meetings.[4]

[3] CSBS. *CSBS Ransomware Self-Assessment Tool for Banks, Version 2.0.* October 24, 2023.
[4] Ibid.