CISO Cross-Industry

Expert Exchange

Q2 Executive summary
April 23, 2024

kyndryl

Overview

During the April 2024 CISO Expert Exchange, industry leaders convened to address the pressing challenges and emerging strategies within cybersecurity awareness and threat mitigation. The discussion delved into the complexities of promoting employee engagement in cybersecurity practices, the need to advance beyond traditional phishing training in response to more sophisticated threats, and the integration of automation to streamline security measures.

Host

Michael Restivo
Kyndryl, USA Vice President – Security and Resiliency

SME

Cory Musselman
Kyndryl, Global Chief Information Security Officer

Key topics

PAGE

Human Risk and Employee Engagement

- There was a significant focus on human risk, with an understanding that while technology and processes are critical, the human element can be both an organization's best defense and its biggest weakness. One member mentioned how they are targeting the help desk as they see a barrage of sophisticated social engineering attacks.

- Strategies to increase employee engagement in cybersecurity were discussed, including making training more engaging through humor, incentivizing positive security behaviors, and providing alternative paths to traditional training methods. One member mentioned that they are creating a balance of consequences around testing, ultimately tying healthy cyber hygiene to employee performance.

- Kyndryl's Global CISO, Corey Musselman, discussed his targeted approach to human risk, focusing on employees with important access, heavily targeted, and not performing well on phishing tests or cybersecurity awareness to make the most out of awareness investment dollars.

- The effectiveness of security education programs was questioned, with a call for better metrics to measure the success and return on investment of such initiatives. In response, some CISOs are not only measuring failure rates but also resiliency rates – the failure rate and reporting rate. There is an expectation that people report that the phish broke through the system, so the security team can react as fast as possible.

> "When measuring the success of our training initiatives, we are paying more attention to resiliency rates than just failure rates. If people are reporting the right things more frequently, that is a better factor on how well your trainings are working."
>
> — Cory Musselman,
> SVP & Global CISO, Kyndryl

Innovations in Security Training

- Creative methods such as comedy skits and interactive formats like escape rooms were used to draw in thousands of employees into cybersecurity education sessions.
- Executive involvement in training sessions was leveraged to show cybersecurity's seriousness and increase employee attention and engagement.
- A 'CyberSafe passport' program was implemented to reward positive cybersecurity behaviors and penalize risky actions, using incentives and disciplinary measures to promote a security-rich culture.
- There was interest in using AI to create engaging and informative security training videos, providing a scalable solution to educate employees on security practices. The AI video-generator tool mentioned during the conversation was Synthesia.

> "Something we did that was surprisingly effective at getting people to understand what phishing really looks like and how to avoid it is we ran a class on how to build a phish. It might sound counterintuitive, but once people understood the mechanics behind a phish, it really helped them understand what to look for."
>
> — CISO Expert Exchange Member

Challenges in Security Communication

- The challenge of communicating cybersecurity information effectively to non-English speaking or diverse linguistic groups was raised, highlighting the need for tailored training that accommodates language barriers.

- The increased sophistication of phishing attacks, comprising of smishing (SMS phishing) and deep fake techniques, was a concern for many, prioritizing the need for advanced defensive strategies, including revamping training campaigns to educate about these newer threats.

- Smishing poses a challenging threat to many on the call considering their lack of control to filter out corrupt texts. Some have worked with carrier providers to ensure timely removal or malicious phone numbers; however, this is not cost-effective. Others have implemented Lookout Mobile Security and Microsoft Defender for mobile.

- The legality of training contractors on cybersecurity was debated, with an interest in how companies navigate co-employment laws to ensure third-party vendors are adequately informed on security policies.

- The necessity of reducing friction in security processes was emphasized, with a call for simplifying security governance and policy to enhance user adoption and limit control circumvention. It was emphasized how important it is for tech and security people to desire governance models with the end user in mind.

> "Just because users are aware doesn't mean they care, and understanding those security controls and the friction we put in place is crucial."
>
> — CISO Expert Exchange Member

The CISO Expert Exchange is hosted by Kyndryl, Inc. Please contact Mike Restivo or Cory Musselman with any questions about Kyndryl or this Exchange.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.
05-13-2024