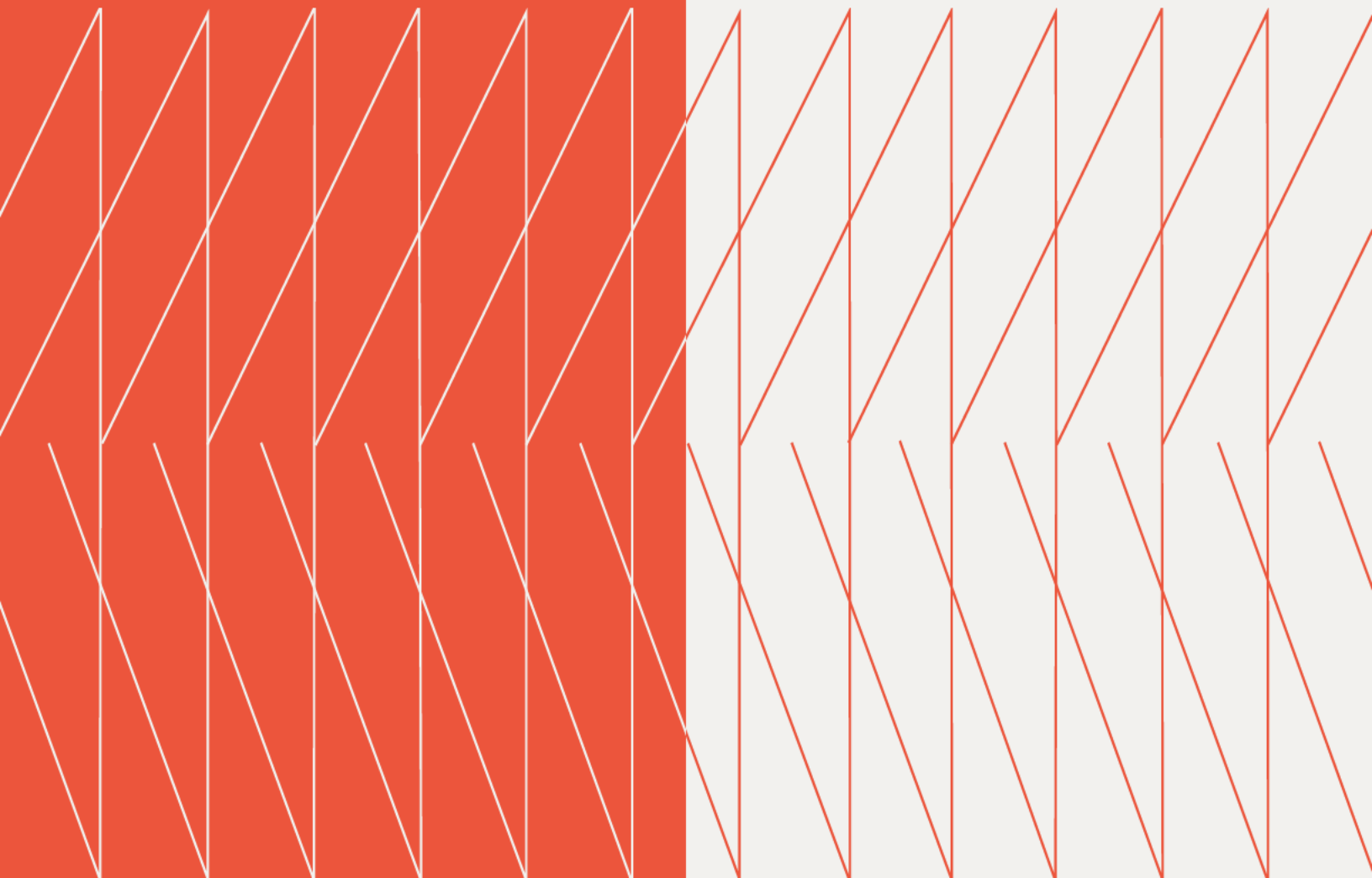
CIO

Expert Exchange

Wednesday,
October 26, 2022

kyndryl

Executive Summary



Host:

Stewart Hyman

Chief Technology Officer, Kyndryl Canada

Shawn McGuire

Chief Technology Officer – Resiliency, Kyndryl Canada

Overview

In this Expert Exchange session, several CIOs from different Canadian industries convened to discuss topics of mutual interest based on an agenda created through advance interviews with participants.

Phishing Campaigns

- Active phishing campaigns conducted on a quarterly basis are useful in reinforcing security training. The success of a phish is not that the employee deleted and ignored a suspicious email, but rather reported it. However, employees report strange things because they know that reporting is part of the exercise, which can lead to reporting false positives.
- Training employees to report phishing emails is a proactive way to educate about security threats, and phishing campaigns can be designed to measure behavioral change. The Outlook view can be formatted in a way to trick an otherwise aware employee to click on an email that should instead be reported as phishing or a security threat.
- A homogeneous set of tools can reduce reporting complexity and benefit both those managing cybersecurity and the everyday employee. The user interface for reporting should not have friction. For example, one should be able to right-click and then report suspected phishing or a suspicious email without clicking on the email or the link.
- "When we're phishing, it's not enough to say, 'This person failed; we have to go educate that person.' There are times when the reason they fail is because we had an incorrect policy around the settings for Outlook which allowed for them to easily accept that email. They didn't recognize that the email was external, so they didn't get notified that the external email could be dangerous."

Zero-Trust

- It can be difficult to convince businesses that there is a security risk associated with simple obsolescence of legacy systems. Pointing out the flaws of legacy systems alongside the benefits of new tools can bring some understanding. Cloud platforms can do much in this area because they create a level of observation not available with the traditional usage of legacy systems. Further the maturity of applications can impact how any applications can be passwordless or which require multi-factor authentication; demonstrating this can make the security risks obvious.
- Zero-trust policies that target desktops and central systems need to apply to mobile computing as well. People who want to use core systems on an iPad, for example, need to verify that the individual using the software is actually the person who should be in that application. Zero-trust reduces incidents greatly but must account for all employee access points.
- Zero-trust considerations also feed into vendor management and outsourcing. The need to apply zero-trust across an environment may lead some organizations to keep everything in-house for control's sake. Otherwise, vendor oversight becomes crucial to ensuring that all applications have a consistent approach to zero-trust.
- "It's not just about controlling the systems, but controlling, almost enforcing, that that amount of zero trust makes it all the way to the mobile device that a person might eventually want use."

Dashboards and Scorecards for Monitoring

- A security scorecard is a good place to start when managing external vendors' attention to security, as some vendors that organizations would think should be highly secure may have low scores. A security scorecard is not the end-all tool, but some leaders keep an A rating on the security scorecard as a requirement. Scorecards can also work backwards by helping vendors figure out how to build their defense plan. A dashboard can be useful for reporting to senior leaders and the board, but the scorecard takes priority.
- While scorecards are useful, there is always the question of the efficacy of security scores, such as from Security Scorecard, a security risk and ratings agency. One security vendor's process for updating their security algorithm took six to eight months—making it always inaccurate, in effect. Security Scorecard's algorithm updates in real time, so that monthly reports always have changes.
- "We used a dashboard to show the effectiveness of the security program; it was infrastructure-based. We measured how many DDoS attacks were prevented and what the firewall caught. We measured the effectiveness of the monitoring and vulnerability management as well. But again, I haven't seen an end-to-end view of a dashboard. It'd be great to see for somebody who has done it."

The Expert Exchange is hosted by Kyndryl, Inc. Please contact Stewart Hyman or Shruti Ojha with any questions about Kyndryl or this Exchange.

kyndryl

2022-06-28