True Office Learning

# Addressing the Human Element of Cybersecurity

**IN THE RACE TO AUTOMATE CYBERSECURITY CONTROLS, HAVE WE FORGOTTEN THAT PEOPLE ARE ULTIMATELY IN THE DRIVER'S SEAT?**

## Overview

- As IT professionals increasingly rely on automation to shore up their cyber defenses, they may be overlooking the importance of "people readiness," or measuring the human element and then responding to it through training.
- Adaptive learning solutions with performance analytics, where an individual's performance drives his/her path through a series of immersive simulations, are now available to help employees not only to acquire the necessary cybersecurity knowledge but also to develop the required neural pathways to override intrinsic human nature.
- Rather than adding more controls, the key to sustained protection lies in addressing the root cause of issues by helping employees to build situational recall and muscle memory of better cyber habits.

With the cyber threat landscape evolving at breakneck speed, many IT professionals see automation, machine learning and artificial intelligence as the best options for mitigating risks and protecting their businesses and their customers. According to the Cisco 2018 Annual Cybersecurity Report, cyber programs are heavily reliant on these advanced technologies, with 39 percent of security professionals reporting that their organizations are completely reliant on automation; 34 percent saying they are completely reliant on machine learning; and 32 percent indicating they are completely reliant on artificial intelligence.[1] Investing in advanced architectures, systems and controls, increasingly enabled by automation, artificial intelligence and machine learning, is certainly an important part of an effective cybersecurity program. So is adopting a standardized cybersecurity framework, such as the one

[1] "Cisco 2018 Security Capabilities Benchmark Study: Defenders report greater reliance on automation and artificial intelligence," Cisco 2018 Cybersecurity Report 2018, Pg. 11, https://www.cisco.com/c/en/us/products/security/security-reports.html

offered by the U.S. National Institute of Standards and Technology (NIST).

But, in the rush to standardize and automate, IT professionals may be overlooking the most important, if not the most vexing, component in an effective cybersecurity program—the humans who work for and engage with the organization. While automation can greatly enhance an organization's ability to identify and detect issues, people are still responsible for remediating and responding to them. Humans are also responsible for running and monitoring the automations.

This suggests that the reflexive preference for investing in technology, rather than in ensuring "people readiness" (i.e., measuring the human element and then responding to it through training), may be off base.

For example, an organization could implement an automated control that flags outbound emails containing confidential information. While it may be helpful to know that someone may be sending protected data outside the firewall, the burden of doing something about it still falls on people. As is often the case, the automation in this instance raises more questions than it answers:

- Did the person who forwarded the email know that it contained confidential information?
- Was s/he acting intentionally or unintentionally?
- Do the people who received the alerts know what to do?
- Is there a standardized framework in place to guide them?
- Do they have the authority, time and capability to investigate and remediate?

The aforementioned Cisco 2018 Annual Cybersecurity Report underscores these human dependencies.[2] Among organizations that receive daily security alerts, the survey found that only 56 percent of alerts are actually investigated. Rather than reactive controls that call upon the organization to "fight fires" as they arise, sustained protection begins with a more aware workforce that prevents sparks from turning into flames in the first place. Addressing the root cause of issues through "people readiness," not just adding another control, is the key to the long-term effectiveness and continuous evolution of an organization's cybersecurity program.

The danger of over-automation has been well-documented of late. It can result in security breaches, operational disruptions, and in extreme circumstances, even loss of life. National cybersecurity frameworks like NIST are the first step in attaining the right balance of technology architecture, automation, and best practices to fortify a company's cyber defenses. Nonetheless, the effectiveness of even those frameworks hinges upon people understanding the technology, monitoring the automation, and following the preferred practices. That's why the human element is an unavoidable part of the mix.

## Those That Do, Learn

When it comes to preparing employees to be good cyber stewards, the typical approach often falls short. Why? Because organizations tend to focus on disseminating information, rather than assessing readiness or influencing human behavior. The former is often based on case studies (i.e., this is what happened at company X, how the actors got in, and how much it cost). The latter is based on learning by doing (i.e., putting employees into situations where they must navigate the environment and make decisions that can be measured.) Similar to simulation training in the military or flight school, adaptive learning solutions with performance analytics are now available to help employees

[2] "Complexity created by vendors in orchestration," Cisco 2018 Cybersecurity Report 2018, Pgs. 48-49, https://www.cisco.com/c/m/en_au/products/security/.../cybersecurity-reports.html

not only to acquire the necessary knowledge but also to develop the required neural pathways to react quickly and thoughtfully at the point of critical decision-making. Immersive training such as this is powerful since it responds to the employees' decisions, challenges them accordingly and assesses their readiness. After all, it has even enabled pilots like Tammy Jo Shults and Chesley "Sully" Sullenberger to land their crippled jets safely. Now, through adaptive learning solutions, any organization can use the same scenario-based principles to help their people develop the situational recall needed to make good decisions and take responsible actions despite stress and other distractions.

Regardless of the demonstrated efficacy of a learn-by-doing approach, many organizations are not aware of its usefulness in creating a culture of cybersecurity. Accordingly, many learning and IT professionals still view cybersecurity preparedness in the same way they always have: as a "once and done" training activity that presents the information based on a series of do's and don'ts. This approach has two flaws: 1) it doesn't allow for active decision making, personalized coaching and collecting behavioral data; and 2) information dissemination isn't enough to build "muscle memory" for evoking automatic reactions in users the next time they are confronted with a dubious decision to "click here" or hit send.

A fully adaptive learning and analytics platform, such as Scholar for Cybersecurity from True Office Learning, addresses both shortfalls. The platform presents a series of immersive training experiences that adapt to the user's role and performance. And, it provides advanced behavioral performance analysis through I.Q., a cloud-based analytics platform, so leaders can assess the level of people readiness and see if the habit patterns within the organization are shifting.

## To Err Is Human

Though immersive training experiences are powerful, they are incomplete without analytics that provide actionable insight and benchmarking. In order to gauge the efficacy of their cybersecurity programs, organizations need to know where their people really stand and what they are likely to do in a given situation. An analysis of behavioral data collected by True Office Learning provides fresh insights into why people "do the crazy things that they do" when it comes to cybersecurity. Consider these statistics:

**I.Q. Analytics data**

**43%** of employees
don't know the proper steps to keep personal devices secure when traveling for work

**34%** of employees
can't identify signs of a possible social engineering attempt

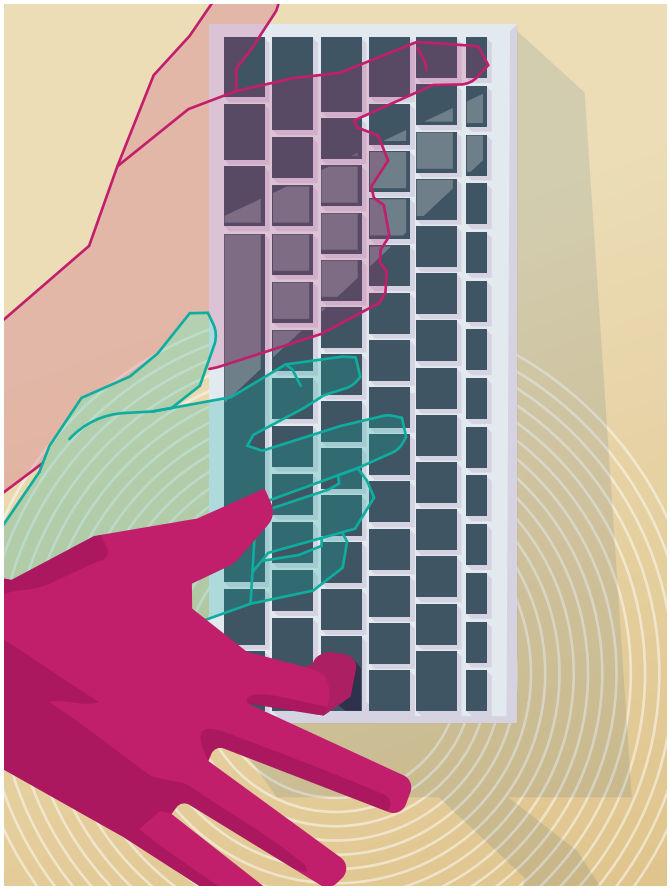
**42%** of employees
are unable to identify data privacy best practices

**22%** of employees
won't report a lost device if they get it back in a few hours, even though information may have been compromised during that time

Overall, the data suggests that most individuals do not have malicious intent. They are not trying to compromise the organization: conversely, they are trying to be helpful. For instance, if people see something suspicious online, they will often try to self-diagnose the problem, rather than escalating the issue through proper channels. Why? Because they don't want to inconvenience the organization without being sure and they don't want to call attention to themselves. But amid the fray, the organization loses precious incident response time.

The behavioral data additionally reveals that people are more likely to expose information when they're under a time crunch or when they're in a role-sensitive situation. For instance, if a sales prospect asks while traveling, "Can I access your computer to print something fast?" A sales rep is likely to comply. This underscores the importance of building situational memory or a habitual response that is strong enough to override intrinsic human nature, which is to be of service. While a person's gut instinct may say "let me help," the right response is to refer the inquiring party to the information security team.

## To Recall Is Divine



Nearly every day a company finds itself on the front page of the Wall Street Journal due to a security breach, struggling to retain customer confidence. Making sure you're not the next IT professional in the hot seat takes more than automating controls; cybersecurity is fundamentally a people problem. This problem can now be minimized at the root through adaptive learning and analytics platforms that help build situational recall and muscle memory of better cyber habits.

These memories, which insert themselves between employees' fingers and their keyboards, are the most potent cyber defense to date.