CORPORATECOUNSEL
NOT FOR REPRINT

How to Strengthen the Human Element in Enterprise Cybersecurity

IT shapes human behavior in today's climate, especially in the workplace. In turn, workforce behavior ultimately determines the effectiveness of IT resources.

By **Rob McCormick** | April 13, 2022

For in-house legal teams not well-versed in technological matters, information technology (IT) can seem like an obscure amalgamation of systems, platforms, applications and networks that are critical to overall success. Many might see workplace culture the same—an essential, albeit opaque, asset often influenced by factors that are hard to understand and track. Interestingly, few seem to associate one with the other.

However, IT shapes human behavior in today's climate, especially in the workplace. In turn, workforce behavior ultimately determines the effectiveness of IT resources. By viewing IT and behavior separately, leaders make it more difficult to get them in sync, leaving their companies' infrastructure more vulnerable in the process.

Consider phishing attacks that empower malicious actors to prey on human error to intercept customers' personal information. According to a Ponemon Institute study, large enterprises experience $15 million in annual losses (https://www.proofpoint.com/us/resources/analyst-reports/ponemon-cost-of-phishing-study) due to phishing, which translates to roughly $1,500 per employee. That figure has risen significantly in recent years, and it will continue to do so unless leaders reconfigure how their employees interact with technology.

The good news? By complementing IT security with staff education, companies not only strengthen security, but also decrease their liability and susceptibility to the consequences of a cyberattack.

Constructing a Human Firewall

Cybersecurity strategies become more comprehensive when carried out by employees who instinctually prioritize network safety. Within most companies, the human workforce is the first line of defense against breachers. For example, an employee who knows how to detect a phishing email can thwart an attack in its tracks and prevent any potential fallout from occurring.

Conversely, those who fall victim to a cyberattack can ultimately cost a business in several ways. If it's determined that someone erred because their client failed to implement reasonable security measures (https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability.), liability comes into play. What does that mean? It means that on top of the short-term remediation costs and potential long-term damage to reputation, companies could be fined or penalized in ways that impair their operability.

Regardless of their understanding of IT or human behavior, most in-house legal teams know that they shouldn't take cybersecurity for granted, yet the evidence shows that many do just that (https://www.helpnetsecurity.com/2021/11/05/not-effectively-stopping-cyberattacks/#:~:text=November%205%2C%202021-,Organizations%20seldom%20prioritize%20cybersecurity
Try these strategies to make cybersecurity a cultural value and lessen company liability:

- **Reduce opportunities for human error.**

Nearly every modern business should implement policies that mandate secure email encryption (https://www.virtru.com/blog/how-to-develop-a-secure-email-strategy/). Because encrypted information can't be deciphered by anyone other than the intended recipients, this represents an additional safety barrier between personal data and potential phishers.

Domain name system (DNS) web and content filtering protect companies from malware by simply blocking access to sites that could pose a threat. Effective DNS filtering can stop most of these threats from ever reaching a company's network. Robust spam filters can block inbound threats by detecting unsolicited, unwanted, or virus-infected emails, leaving companies and staff less vulnerable to breaches.

- **Invest in employee training.**

Considering that human error is a signiffcant contributor to 5% of cyberattacks (https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html), there's no reason not to require every employee to complete some annual security awareness training. Online training courses ofiered by jnowBeS (https://www.knowbeS.com/), Rapid (https://www.rapid.com/), and limecast (https://www.mimecast.com/), among others, can be conffgured to meet requirements speciffc to difierent industries and businesses. Furthermore, they can provide engaging educational content that teaches a team key concepts and actionable best practices.

Plus, by making security training an official company policy, leaders can likely reduce their business's liability if a breach does occur by showing regulators that the proper guardrails were in place beforehand. Companies that are unable or unwilling to consider companywide training should at least develop their own internal evaluation method to ensure employees stay updated on how to carry out their responsibilities securely.

For example, this assessment could involve asking an outside vendor to send emails with elements of phishing in them and requiring employees to identify red flags and potential liability issues. Even if it results in a brief slowdown in productivity, closing any workforce knowledge gaps as quickly as possible will pay dividends over time.

- **Tie security to the bottom line.**

While a culture of security must start from the top, the attitudes and practices that are part of that culture must be adopted across the enterprise. In some cases, leaders might receive pushback from managers who are already busy enough. In those cases, illustrate the large-scale ramifications that come with not paying attention to cybersecurity.

To help them understand the importance of a strong security posture, educate them on how breaches impact core business functions such as customer retention and product development, along with the potential legal ramifications that stem from a lack of preparation. The tendency is to view security solely as an IT problem, but nearly every business unit will be affected in the wake of a cyberattack.

A comprehensive security program addresses the technological *and* human elements of cybersecurity, ensuring that these resources can prevent attacks rather than enable them. As threats continue to grow in number and complexity, leaders must adapt their IT assets and workforce accordingly. With malicious actors adjusting their methods by the minute, complacency is not an option.

Rob McCormick *is the CEO at Avatara* (https://avataracloud.com/)*, a St. Louis-based company whose CompleteCloud Platform offers small to midsize businesses across the nation a revolutionized approach to buying, utilizing, and maintaining their IT environments. McCormick resides in St. Louis.*