The Finance Factor: Digital Security in the Age of Human Capital
By ADP Spark Team, DATA SECURITY

Digital security is paramount in a connected world where the human attack surface outpaces traditional network risks.

The "human attack surface," defined as hackers who now attack people instead of devices, is on the rise. Why does it matter for finance leaders? Because any staff member with access to corporate networks — effectively *everyone* — represents potential threat, and potential loss. As We Are Social notes, there are currently 3.77 billion active internet users; the steady proliferation of mobile and always-connected devices will only push this number higher in the coming years.

For finance decision-makers, the path is clear: Spend on digital security before attack surfaces get out of hand. The challenge? Knowing where to spend security dollars to both limit total risk and align with ROI goals.

Don't Wait, Educate

The first step is to educate employees. This comes with upfront costs such as paying for expert training, offering online education and keeping track of completed courses and certifications. But it also comes with big benefits. For example, CSO reports that 91 percent of cyberattacks start via email. Why? Because employees are conditioned to respond quickly if they believe emails are from upper management or important business partners and may inadvertently leak critical information or provide secure access details. Educating employees to avoid suspicious emails and immediately report phishing attempts both hamstrings most low-level attacks and helps create a corporate culture of discourse rather than secrecy. Cost-wise, finance leaders must be prepared to spend on regular (every six months or so) retraining for employees.

Doubling Down on Digital Security

According to CSO, ransomware costs pushed into the *billions* through 2017, a 15-fold increase over 2015. And the numbers are only escalating, with some security firms predicting ransomware attacks every 14 seconds over the next few years. For organizations looking to shore up digital security, the growing problem of ransomware means that employee training alone isn't enough; cybercriminals are now employing both brute-force methods — such as distributed denial-of-service (DDoS) attacks to distract from malware infections — and sophisticated threat vectors like fileless malware to compromise corporate systems.

As a result, cybersecurity budgets might include money earmarked for advanced security solutions capable of analyzing application runtime environments, automatically quarantining potential threats and actively learning from new attack patterns. The price tag here isn't small, making it a difficult ROI conversation and one better framed as

reduction of risk: While security solutions won't "make back" the money spent on purchase and installation, they can significantly reduce the amount of money lost over time to stolen data, network cleanup and system remediation.

Keeping Track

Also worth your time are HR management solutions capable of tracking employee network behavior in real time. Here, the goal is to help limit the potential spread of cyberissues and curb risky behavior such as the proliferation of "shadow IT."

Cloud-based offerings now make it possible to link digital security efforts across departmental silos, but the bigger challenge is ensuring that employees understand the purpose of the system, how it works and what specific consequences will result if they choose risky online behaviors. Finance leaders can position new HR tools as a win-win across the organization: With employees on board, IT can leverage these solutions to start meaningful discussions of application use and employee permissions, while HR staff gain a detailed record of online behavior to help inform ongoing training and speak to specific staff issues.

"Making sure employees know what is expected of them and what the consequences are for inappropriate behavior is critical – and its not just a security responsibility," said Kim Albarella, senior director of ADP's Global Security Organization.

The CFO and HR functions play a key role in helping to communicate expectations and kick-start those conversations – and these tools can help them with that."

Digital security is paramount in a connected world where the human attack surface outpaces traditional network risks. For finance leaders, it's worth deploying budgets across employee education, advanced security software and real-time HR tools.

https://www.adp.com/spark/articles/2019/08/the-finance-factor-digital-security-in-the-age-of-human-capital.aspx#