FS-ISAC

Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – January 2022

Global Cybersecurity Skills Shortage Falls for Second Consecutive Year

A **study** performed by (ISC)^2 highlighted that of the 4,700+ global participants polled, results revealed a **skilled workforce that decreased** from 3.12 million last year to 2.72 million this year. The global workforce grew to approximately 4.2 million, although there are workforce gaps in this number. The study broke down the results into three regions: APAC, which had the largest gap of the regions, Europe, and North America. There is cause for an organization to pay attention as staff shortages could have direct impact on their business: misconfigured systems, patching delays, and process oversights to name a few. One of the positives coming from the poll is 77% of those who responded say they are either satisfied or extremely satisfied with their jobs. To further engage these skilled employees and future employees, organizations should look to "invest in their development and embrace remote work as an opportunity".

Cyber Awareness Training Needs to be Relatable for Employees to Remain Vigilant

Employees are considered to be the first line of cybersecurity defense for any organization, yet it's estimated that **95% of all cybersecurity breaches** are due to human error. Cybersecurity training needs to engage and stick with employees as duplicate passwords continue to aid in approximately 73% of all accounts being guarded. Organizations should update current training protocols as videos that were once considered useful years ago no longer work for today's workforce. One way an organization can demonstrate awareness training is to make it relatable to the employee and their personal social media security. An engaged and well-versed employee will become a much stronger defense for an organization.

Cybersecurity Sidelined by Other Goals When Communicating to the C-Suite

The **importance of keeping an organization's senior executives and Board informed** on cybersecurity risks is not only essential but a necessity. Reports show that roughly 50% of IT leaders and 38% of business decision makers feel C-Suite executives truly understand the risks to their organizations, as their focus usually goes to goals and revenue projections, to name a few. Once a Board understands the implications and scale of a breach will organizations be able to prioritize and proactively invest in sophisticated cybersecurity tools.

Why Zero Trust is Key for Today's Remote Worker

Organizations are trying to adapt to the reality of a workforce that may work in the office, work remotely, or both. With that reality comes a need to ensure their networks and employee devices remain secure. While VPN was a go-to model a few years ago, the need for further security options now lies in a **Zero Trust Network Application** (ZTNA), which enables the organization to trust the transactions versus the entity or organization. A great way of looking at ZTNA is that trust is earned, not given, each time an employee requests access to an application. Organizations should take note that ZTNA will allow them to be empowered to improve operations with security that is more streamlined.