Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – September 2021

Risk Assessment Needs a Closer Look

The importance of **risk assessment** goes much deeper than many organizations might realize. CEOs and Boards of Directors must understand the risks to their organizations, which starts with a risk assessment. Organizations must identify, prioritize, and then know how to mitigate risks to have a comprehensive plan. What most risk assessments don't include are specific security controls, which do not allow an organization to convert policy plans into action. To get started on a risk assessment, start with the following: Keep a risk library tied to strategic objectives, map controls to risks automatically, and ensure you know your controls are operational in real-time.

SEC Sanctioned Eight Firms with Deficient Cyber Procedures

Last week, the Securities and Exchange Commission (SEC) sanctioned eight firms **for failures in their cybersecurity policies and procedures**. The failures resulted in email account takeovers exposing personal information of thousands of customers and clients at each firm. Most of the firms that were fined was because a third party took over a majority of the firm's cloud-based email accounts of company personnel, exposing personally identifiable information (PII) to customers and clients. None of these account takeovers were protected in a manner consistent with the policies defined by the firm. The orders against these firms were that they violated Rule 30(a) of Regulation S-P, also known as the Safeguards Rule, which is designed to protect confidential customer information.

Costs of Phishing Attacks Nearly Quadrupled in Six Years

The **costs of phishing attacks** on US organizations show an average loss of $14.8 million annually, or roughly $1,500 per employee, which is almost quadruple the amount since 2015. While phishing has led to costly cyberattacks, business email compromise (BEC) is one of the most expensive threat types with more than $1.8 billion stolen from organizations. **Ransomware** has also experienced a 64% increase in attacks, year-over-year. Many employees within affected organizations may not realize that costs stemming from ransomware attacks include not only the ransom paid but rather lost productivity and remediation of the issue. Employee training remains paramount to reduce these events as security awareness training has shown to reduce phishing expenses by more than 50%, on average.

FINRA Report: Cloud Computing in the Securities Industry

Last week, the Financial Industry Regulatory Authority's (FINRA) Office of Financial Innovation **released a report** to better understand the implications of cloud computing on the securities industry. The report states that firms have identified certain challenges investment firms faced during their cloud migrations, including developing the appropriate protocols and skill base to facilitate establishing and maintaining cloud security, sufficiently changing organizational processes and firm culture to take advantage of the offerings presented by a cloud platform, while limiting the potential for vendor lock-in risk with a cloud provider. The report summarizes key findings from the regulations review in three sections, covering an overview of cloud computing, experiences with cloud adoptions, and regulatory considerations for cloud computing.