COSMOS
Navigate the Compliance Universe

CEP Magazine - March 2023

Jamie Smith (hello@s-rminform.com; linkedin.com/in/jamie-smith-500174103/) is Board Director and Head of Cyber Security at S-RM in London, England, UK.

As cyber threats rise and budgets fall, what can compliance professionals do?

By Jamie Smith

In recent years, C-suite leaders and senior IT experts have witnessed a rise in cyberattacks against their organizations, with 2022 seeing one of the highest spikes yet. In fact, according to our 2022 *Cyber Security Insights Report*, serious cyber incidents have increased 25% yearly across both the United States (US) and the United Kingdom (UK), naturally bringing significant ramifications for compliance professionals.[1]

Despite rising threat levels, companies' cyberattack budgets often do not reflect this growing risk. Cybersecurity funding is expected to increase only 11% on average by 2025, and perhaps even more concerning in the same period, 13% of UK organizations are even expecting budget cuts in cybersecurity measures.

If businesses are to deal effectively with serious cybersecurity incidents, compliance professionals, IT experts, and business leaders must all work together and prioritize cybersecurity. We must aim for a holistic strategy that includes insurance, security, and response strategies, with regulatory compliance running through each area.

Proactive versus reactive

All too often, companies take a reactive stance to cyberattacks rather than a defense-in-depth preventive approach. Not only does this potentially jeopardize reputation and the bottom line, but it also invites greater scrutiny from regulatory bodies. According to our cyber report, a third (33%) of those who experienced a cyberattack in the last three years reported they were subsequently subjected to regulatory investigation, and more than a quarter (28%) received a regulatory penalty of some kind. These are not figures that a compliance expert will welcome reading.

Organizations should always take a proactive approach to cybersecurity threats to mitigate regulatory risks at a time of falling budgets. But what does that mean in practice?

The first step to best defend against malicious actors and threat groups is to develop a stronger understanding of a business' internal vulnerabilities before they become compromised.

Compliance teams can achieve this by replicating a threat actor's actions in a simulated attack or incident. This allows them to better understand which areas of cybersecurity can be improved in the event the real thing is to happen. Through these test protocols, businesses can also calculate the associated costs of a cyber incident; business leaders should evaluate the regulatory compliance implications of these mock attacks as part of this testing.

Undertaking a stress test with a firm eye on General Data Protection Regulation, Markets in Financial

Instruments Directive, Markets in Financial Instruments Regulation, or Competition and Markets Authority regulations, as a few examples, will ensure that these regulatory considerations are front of the queue when it comes to evaluating what processes may need improvement.

In addition to general testing, deploying customized penetration testing techniques is hugely beneficial to organizations in identifying both internal and external vulnerabilities. In broader terms, these take the form of mock attacks on your infrastructure and network that are "personalized" against your own business, reflecting the level of research and intelligence that goes into more targeted incidents.

After such a customized test, businesses can better analyze the implications for their regulatory compliance—not to mention better consider the best protection for the assets most critical to the company's success.

Tools are also available to give compliance teams a "score" over their company's cybersecurity maturity. As part of the National Institute of Standards and Technology (NIST) Cyber Security, CIS-18, and ISO27001:2022 industry frameworks, it's possible to assess cybersecurity maturity across every asset and infrastructure, resulting in an overall maturity score that shows where improvements are needed. Should an incident occur, and a regulatory body becomes involved, showing this score and detailing the efforts made to improve it is a powerful demonstration of good intent.

Going beyond these frameworks, taking a proactive approach is also possible through open-source intelligence, known as OSINT. OSINT programs rely on expert intelligence-gathering from a variety of sources, including even scanning dark web forums for discussions about a company and whether credentials or sensitive information have been leaked.