Report on Supply Chain Compliance Volume 2, Number 4. March 07, 2019
The rise of cybercrime and the need for cyber resilience

In the last five years, cybercrime against both public and private entities has experienced a marked increase. According to a report published by Accenture, "Cost of Cyber Crime: Financial Services," costs for the financial sector have risen 40 percent between 2014 and 2017, and the number of reported breaches per financial services firm has grown from 40 breaches in 2012 to 125 breaches in 2017. In 2018, cybercrime incidents continued to increase, as did the financial toll in terms of disruptions to business supply chains and business continuity.

According to a report by Hackmageddon cybercrime has increased as a percentage overall, while cyber espionage, "hacktivism" and cyber warfare have not. Malware is the top attack technique (34.4 percent), followed by account hijacking (18.2 percent) and targeted attacks (13 percent). Since cybercrime is the most significant type of attack, it follows that financial damage (both direct and due to reputational damage) will have increased with the increase of attacks. Some of the costs that entities can incur include remediation costs for stolen assets and information, increased cybersecurity protection costs, litigation and legal fees, reputational damage, increased insurance premiums, and damage to long-term shareholder value.

"Cybercrime has been around since we've had computers," said Mark Lanterman, the Chief Technology Officer of Computer Forensic Services. "But we have seen a rise in our business, and much of that is due to the rise in 'hacking as a service.'" Hackers are now selling their services, or ransomware, on the open market to individuals who know much less about cybercrime, but have a motive and funds to pay for an attack. A hacker in Minnesota, USA, for example, was able to shut down the court system for several days for less than USD 500, and investigators were able to trace the attack to him, but not to the hacker who sold the services.

This document is only available to subscribers. Please log in or purchase access.

Purchase Login