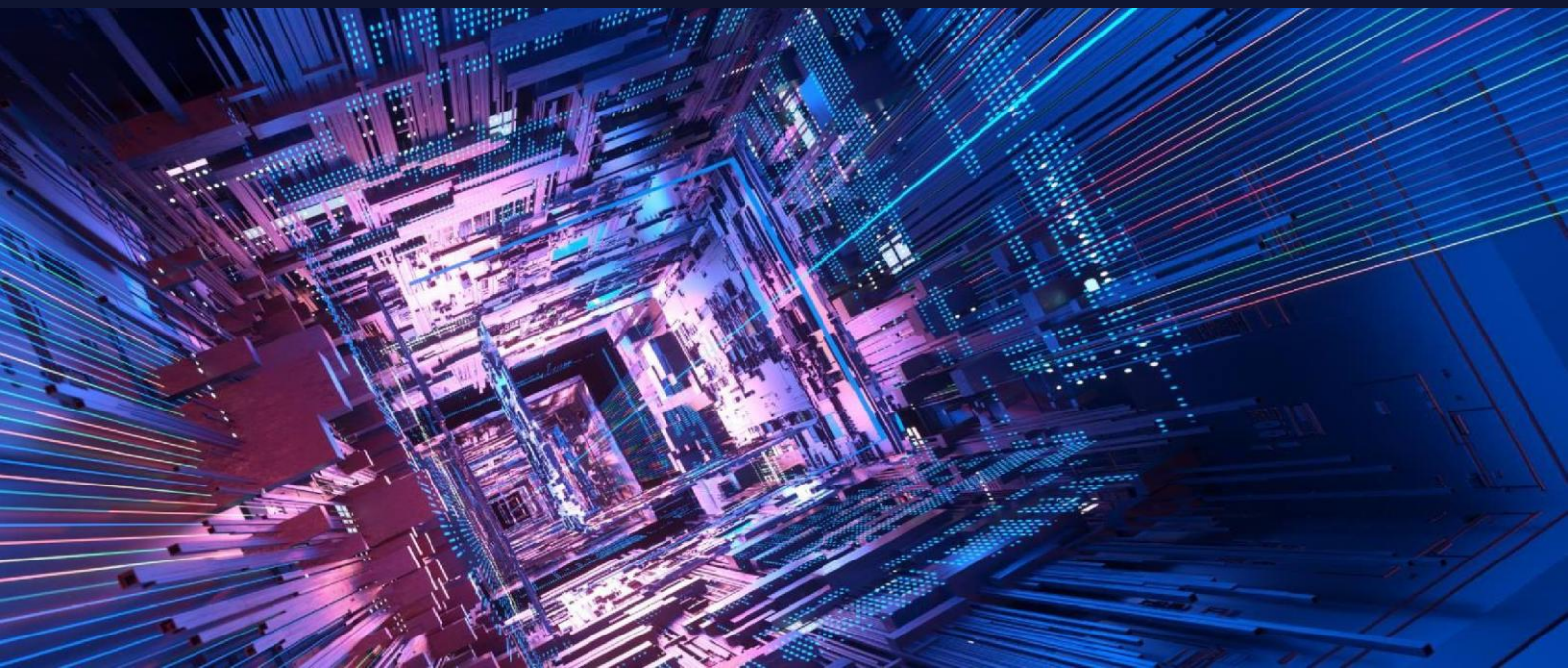

The Ever-Evolving Cyber Threat

Cyber criminals are constantly evolving their tactics to find new opportunities to commit fraud, hold data or systems hostage for ransom, or steal sensitive information that they can exploit or sell. Increased reliance on digital infrastructure can transform our lives and businesses, but it also requires increased vigilance.

While the context may change, many of the fundamentals of cybercrime do not. Criminals predominantly seek unauthorized access to systems and information in order to exploit it in some way, such as initiating a fraudulent payment, exfiltrating data, or disrupting business.

As companies become savvier at mitigating threats, cybercriminals become savvier at changing the game. For instance, after a dramatic increase in ransomware attacks, which largely rendered data unavailable until a ransom had been paid, many companies began to ensure they had backup data sources available to ensure continuous operations. In response, rather than threatening to lock companies out of their systems, many cybercriminals have pivoted to demanding a ransom in exchange for a promise not to release or sell sensitive data. Client data can be sold (on the dark web) to facilitate fraud, identity theft, account takeover, or as weapons in broader social engineering attacks (using privileged information to gain unauthorized access elsewhere). This trend reflects the increasing specialization of cyber criminals, who frequently trade services (or access to a specific company) with others.

In addition to financial risks associated with potentially making a ransom payment and incurring expenses associated with incident response, cyberattacks can cause great reputational harm and erode customer trust, impacting future business. A leak of payroll information could undermine staffing and the company's ability to compete with other firms. Cyberattacks could compromise trade secrets, material nonpublic information, confidential financial reports, and other sensitive data. It is therefore important for businesses to not only consider how they store their sensitive data (in order to ensure its security) but also to have a clear strategy for identifying the extent to which data is compromised in the event of a successful attack so that impacts can be adequately assessed in light of ransomware demands or other fraud risks.

Translating cyber risks to business risks

Cyber threats can come in a variety of forms and their business implications also vary dely.

CYBER THREAT: BUSINESS E-MAIL COMPROMISE

The average loss in Business Email Compromise (BEC) scams exceeds $135,000 according to the FBI's Internet Crime Complaint Center. Increasingly, threat actors are enhancing their attacks using deepfake technology, including AI-generated voice and video impersonation to deceive employees and executives.

Business Impact: A BEC attack can potentially undermine the viability of the business. Deepfake - enabled attacks further elevate this risk by enabling highly convincing impersonation of senior executives (e.g., CEO/CFO), increasing the likelihood of fraudulent transactions and unauthorized actions. In addition, corporations may subsequently need to hire investigative teams and update their infrastructure (or accelerate existing investment) to prevent similar attacks in the future.

CYBER THREAT: CLIENT DATA COMPROMISE

Business Impact: When client data containing personally identifiable information is acquired or leaked by cyber criminals, companies can face fines from regulators or other government bodies, be subject to class-action lawsuits brought by impacted clients and accrue significant expenses to identify and notify data subject. Costs are usually based on the number of data subjects impacted and can be a function of gross revenue.

CYBER THREAT: CLIENT DATA COMPROMISE

Hybrid and work-from-home working models have exacerbated the risk of cyberattacks. People are generally the weakest link when it comes to cybersecurity, with many successful attacks resulting from individuals inadvertently clicking on a malicious link or accidentally compromising their credentials, rather than as a result of system weaknesses. Remote working has increased the number of successful cyberattacks.

Business Impact: These types of threats can be the gateway to fraud (e.g. paying an incorrect invoice) or provide the attackers access to the infrastructure that cyber criminals can exploit to take down a business or steal sensitive data.

What does an effective cyber defense strategy look like?

Most businesses can expect to be targeted in a cyberattack at some point. Adequate preparation can greatly improve a company's ability to prevent, detect, respond to, contain, and recover from an attack.

Companies need to develop a multipronged, holistic cyber defense strategy covering readiness, response and recovery.

Readiness

Companies need a layered defense using sophisticated and regularly updated tools. Skilled personnel are important to prevent cyber-attacks, including a strong IT and IS function, as well as partnerships with external security firms and law enforcement. Necessarily, cybersecurity requires monetary investment . However, an ounce of prevention is worth a pound of cure when considering the costs of responding to a cyberattack, the size of which can be an existential threat for some companies.

Best Practice: Ensure that your cybersecurity strategy contemplates things like access controls (including strong password policies and limited entitlements to systems and data), encryption of data when it is stored in your systems or moved between parties, malware prevention solutions, policies for protecting your data from human error and malicious actors (for example, preventing data from being removed from the business network), identification of possible threats with tailored strategies for mitigating them, and development of strong employee training programs across the organization. Training to raise risk awareness is absolutely critical. Companies should prepare for cyberattacks through tabletop exercises and simulations so that if cyberattacks occur, people know what to do. Typically, these exercises should consider warning signs of an attack, escalation channels, strategies to continue business operations if there is system or data unavailability, whether there is a need to bring in a third-party cyber response firm, whether to hire legal counsel, etc.. You should also consider whether it might be prudent under the circumstances to notify a bank in order to restrict access to online banking. Your third parties, including supply chain partners, should also conduct similar risk analyses and training.

Response

Your response strategy should include tools to detect a cyberattack as early as possible and communicate that information to all relevant parties (including supply chain partners), so that action, such as systems updates, can be taken quickly. Your cybersecurity program should also be developed to respond promptly to alerts sent by third parties.

Best Practice: Time is of the essence when responding to a cyberattack. This is especially true in relation to payment fraud: after 48 hours, there is little chance of recovering funds. While 48 hours may sound like plenty of time, not every cyber event is as perceptible as a ransomware encryption screen; some cyberattacks may look like a slightly unusual transaction that could take some time to investigate internally. Preparing the team to immediately contact payment fraud teams and other relevant parties and knowing what to say and who to ask for, can therefore be critical.

Recovery

Companies should have a clear business recovery plan to get back to restore functionality as soon as possible. This plan should include redundant data or systems that can kick in when primary systems and data sources are unavailable.

Best Practice: Evaluate whether it makes sense for your organization to purchase cyber insurance and be sure to have experts (like forensic firms and legal counsel) on retainer as part of a response strategy.

The role of law enforcement

Reporting a cyberattack to law enforcement is sometimes seen as a burden for companies. Moreover, many companies may be worried about negative publicity.

Nevertheless, reporting a cyberattack to law enforcement could be beneficial in assisting with your investigation, demonstrating good-faith efforts to address the issue, making an insurance claim, and, potentially in the recovery of stolen funds. The possibility of dismantling criminal infrastructure is greatly improved when law enforcement receives notice and information from victims.

Reporting a cybercrime may also assist law enforcement in identifying of patterns of activity. Reporting a crime can enable parallel investigations to be connected, facilitating coordinated international action and helping to prevent future cyberattacks.

Law enforcement engagement can be useful in other ways. Many national agencies provide resources for businesses to improve awareness. In addition, Europol's European Cybercrime Centre operates the No More Ransom project, which is operated with other partners. As well as providing information to help organizations to prevent cybercrime, the portal offers 132 decryption tools (enabling users to gain access to their data) that are regularly updated; support is available in 37 languages.

CONCLUSION

The scale and sophistication of cybersecurity threats can seem daunting, but even modest adaptations can make large differences in preventing, detecting, and responding to cyberattacks.

Organizations do not need to face the cyber challenge alone. National and international law enforcement agencies often provide resources to help organizations plan their defense strategies and raise awareness of risks. Partners such as banks can also do much to help. If an organization suspects that a cyberattack has occurred or detects an anomaly that might be indicative of a cyberattack, it should contact its bank immediately to monitor the account or shut down transactions until the risk is addressed.

Citi is actively working to improve institutional awareness of cyber threats. Citi has created a portal for clients to share fraud prevention best practices and learn about actual cyberattacks and responses through case studies. Citi also offers a range of resources to help organizations train their staff about attack vectors that are relevant for the treasury and finance functions. As well as practical insights, the portal provides information about the importance of creating a culture of empowerment and vigilance. Citi also issues regular communications to clients about cyber vigilance, current threats and best practices.

In addition to supporting clients directly, Citi invests consistently in its cybersecurity capabilities. In recent years, new risk detection capabilities have been added to CitiDirect Online Banking that leverage behavioral analytics, such as identifying devices used to log in to an account or a user's typical typing patterns. If unusual behavior is detected, users are asked to re-authenticate and are sent a notification via e-mail or SMS. Biometrics are now available for logging in to CitiDirect in most countries, making use of smartphones' biometric capabilities to enable them to securely access the portal on the desktop. Citi has introduced new encryption algorithms for security certificates to stay one step ahead of cyber criminals. And, of course, Citi takes its own cybersecurity extremely seriously, conducting regular training for all staff on risk reduction, data hygiene, incident detection, and other relevant topics.