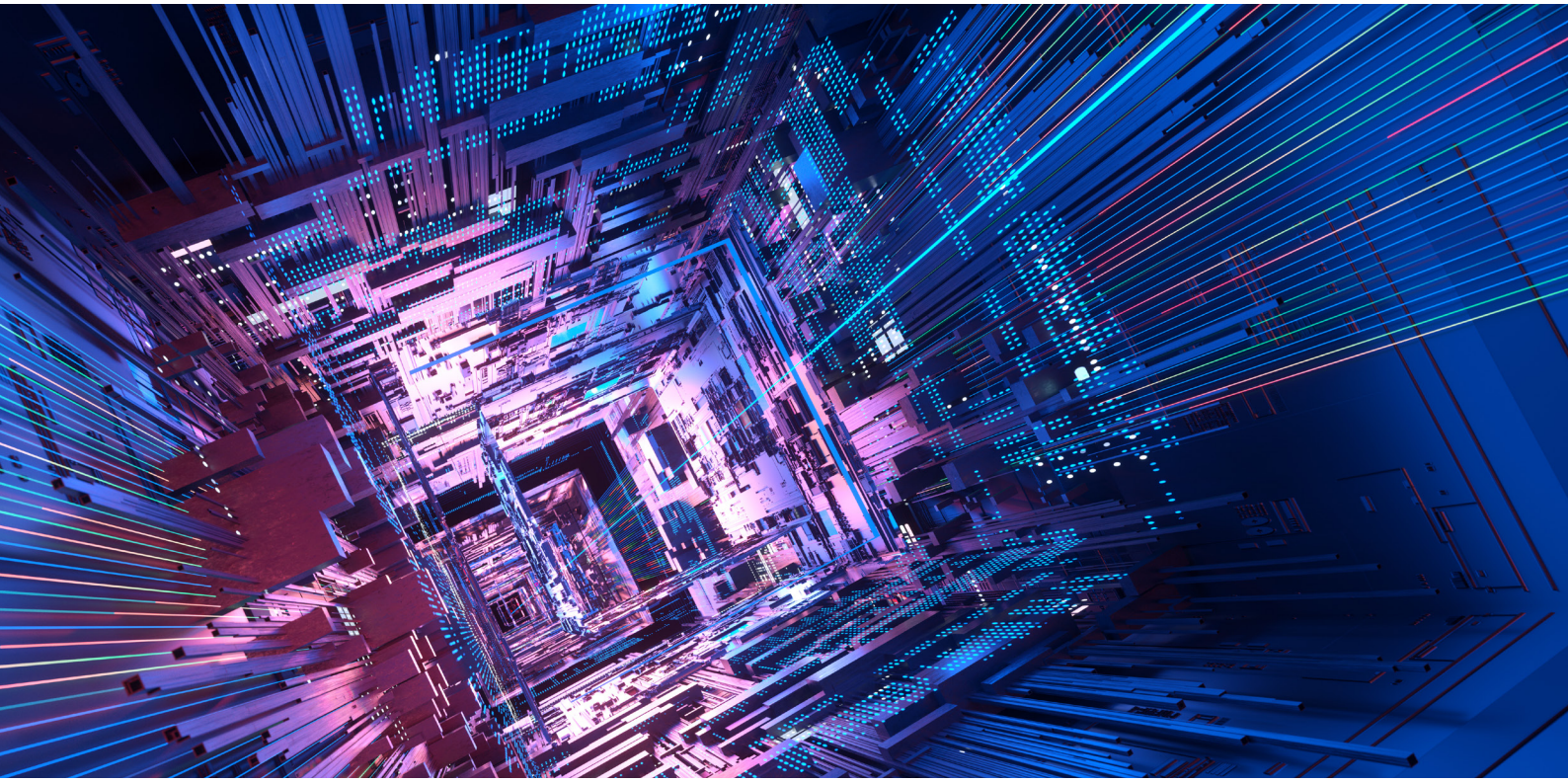

The Ever-Evolving Cyber Threat

Cyber criminals are always looking for opportunities to target institutions in order to commit fraud, ask for ransoms while holding systems/data hostage, or stealing sensitive information. Increased reliance on digital infrastructure, a fundament element to innovation in the global financial system, requires increased vigilance for good cyber-hygiene.

These developments reflect the fact that while the context may change, many of the fundamentals of cyber-crime remain relatively constant. 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). At the same time, while the basics remain the same, different types of cyber threats fluctuate in severity – ransomware has grown significantly as a threat in recent years, for example.

Criminals also adapt their strategies to new circumstances. For instance, in recent years, as the threat from ransomware has grown, many companies have created backups so they can continue to operate without paying a ransom. In response, rather than threatening to lock companies out of their systems, many criminals have pivoted to threatening to release sensitive client or other data. Client data can be sold (on the dark web) to facilitate fraud or as part of a broader social engineering attack (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.

Alternatively, having captured sensitive data, it may be held to ransom, exploiting companies' concerns about reputational damage. A leak of payroll information could undermine staffing and the company's ability to compete with other firms, for instance. It is therefore important for corporates and other entities 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. That way, threats can be adequately assessed in the light of ransomware or other fraud strategies.

Translating cyber risks to business risks

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

CYBER THREAT: BUSINESS E-MAIL COMPROMISE

Attacks such as business email compromise can result in significant losses: A report from the FBI on BEC found that losses totalled 43 billion for the time period between June 2016 and December 2021.

Business Impact: A BEC attack can potentially undermine the viability of the business. In addition, corporates may subsequently need to hire investigative teams and may have to update their infrastructure – or accelerate existing investment – to prevent a similar attack in the future.

CYBER THREAT: CLIENT DATA COMPROMISE

Where client data containing personally identifiable information is acquired or leaked by cyber criminals.

Business Impact: companies can face fines from regulators or other government bodies. Costs are usually based on the number of records and gross revenue.

CYBER THREAT: SOCIAL ENGINEERING

The new hybrid working model adopted by many companies in the wake of the pandemic has exacerbated business risk from cyber-attacks. People are generally the weakest link when it comes to cyber events, with a successful attack being the result of individuals clicking on a link or accidentally compromising their credentials rather than as a result of systems weaknesses. With people working remotely, the likelihood of attacks being successful has increased.

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

What does a cyber defense strategy look like?

While cyber threats can be considered generically alongside other business risks, such as the dangers that result from a natural disaster, corporates also need to address their unique characteristics. Unfortunately, it is a business reality that most companies will suffer a cyber-attack at some point. Adequate preparation can make a big difference to a company's ability to 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 attack, including a strong IT and IS function, as well as partnerships with external security firms and law enforcement. Necessarily, cyber security entails a business cost. However, this is dwarfed by the potential cost of a successful cyber-attack, the size of which can be an existential threat for some companies.

  Best Practice: Identify possible threats, and develop strong employee training programs across the organization. Training to raise risk awareness is absolutely critical. Companies should prepare for cyber-attacks through tabletop exercises and simulations so that if attacks occur, people know how to respond. Typically, this information should include details such as who should be contacted if office infrastructure is unavailable. For example, it may be important to notify a bank in order to restrict access to online banking. It is also important that third parties, including supply chain partners, conduct similar risk analysis and training.

- **Response:** Mechanisms to detect an attack 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. Mechanisms to respond promptly to alerts sent by third parties also need to be put in place.

  Best Practice: Time is of the essence when responding to an attack. This is especially the case in relation to payment fraud: after 48 hours, there is little chance of recovering funds. While 48 hours sounds like a long time, not every cyber event is as blatant as a ransomware encryption screen; some attacks may just be a slightly unusual looking transaction that may take some time to investigate internally. Preparing the team to be able 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 need a clear recovery plan to get back to business as usual by making use of a data back up or alternative facilities, for example.

  Best Practice: Evaluate cyber insurance and have experts on retainer as part of a response strategy that can play an important role in mitigating damage.

The role of law enforcement

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

Nevertheless, reporting is essential in order to start investigations and identify perpetrators (and also potentially, to make an insurance claim or recover fraudulent funds transfers). Criminal infrastructure can only be taken down if law enforcement has clear details from the victims of a crime.

Reporting a cybercrime will not only aid the investigation of a specific incident but – given the international nature of cybercrime – allow the identification of patterns by agencies such as Europol. Reporting a crime can enable different investigations to be connected, facilitating coordinated international action and helping to prevent future attacks.

As well as sharing information, law enforcement 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 often seem daunting for businesses; certainly, it is a growing problem. But by staying vigilant, making modest adaptations as threats evolve, and – most importantly – implementing some basic practices across the organization, it is possible for corporates, public sector entities and others to reduce risky behavior and mitigate many threats from bad actors.

Companies do not need to face the cyber challenge alone. National and international law enforcement agencies often provide resources to help corporates plan their defense strategies and raise awareness of risks. Partners such as banks can also do much to help. Most obviously, when a company suspects that a cyber-attack has occurred or spots an anomaly, they should contact their bank immediately: far better to have a false alarm than to overlook a real attack.

Citi is actively working to improve institutional awareness of this threat. Citi has created a portal for clients to share fraud prevention best practice and learn about actual cyber-attacks and responses through case studies. Citi also offers a range of resources that act as an end-to-end toolkit to help corporates train their staff about attack vectors that are relevant for the treasury and finance functions. As well as practical insights, the portal provides information that explains why it is important to create a culture of empowerment and vigilance so that employees do not process payments if they feel uncomfortable. Citi also issues regular communications to clients about cyber vigilance, current threats and best practices.

As well as supporting clients directly, Citi invests consistently in its cyber security capabilities. In recent years, new risk detection capabilities have been added to CitiDirect Online Banking that use behavioral biometrics, such as identifying the device used to log in or a user's typical typing patterns. If unusual behavior is detected, users are asked to re-authenticate and sent a notification via e-mail or SMS. Biometrics are also available to be now used 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 cyber security extremely seriously, conducting regular training for client-facing staff on risks and who to contact within the bank if they are concerned about cyber threats.

www.citibank.com/tts

CBS36928 10/22