Tackling Fraud and Cybercrime

The scale of cybercrime is astonishing. Global losses in 2020 topped $1 trillion – a 50% increase since 2018.[1] The FBI received 1 million complaints about cybercrime from March 2020 to May 2021, a level previously recorded over three years.[2] About three-quarters of organizations were targets of a payments fraud attack in 2020.[3] And the number of zero days, or previously unknown security vulnerabilities, in 2021 was almost double the total in 2020.[4] Cybercrime is now truly global: many U.S. attacks are actioned from the other side of the globe, making prosecution difficult.

Nic White
Global Fraud Risk Management Director
Citi Commercial Bank

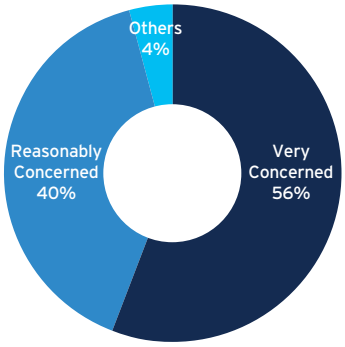
Estelle Shaw-Latimer
Digital Platforms & Transformation Director
Citi Commercial Bank

"While the shift to remote working during COVID-19 increased the world's vulnerability, the volume of cyberattacks has grown steadily for many years," explains Ann Barron-DiCamillo, Global Head of Cyber Operations at Citi. "One reason is that there is greater information sharing among cyber criminals than in the past, when sophisticated techniques were only available to nation state actors; now they are available as a service on the dark web. As importantly, the cost of infrastructure is now so low that it can simply be abandoned once a threat has been identified and made non-malicious."

A recent poll of almost 200 Citi Commercial Bank clients conducted during a webinar showed that cybercrime is a major concern for companies: 56% of respondents said they were very concerned while 40% were reasonably concerned. Given the changes in the threat landscape and the increasing number of businesses targeted by cybercrime – PwC's Global Economic Crime and Fraud Survey showed that 47% of businesses globally (and 56% in the U.S.) have lost money to fraud in the last two years[5] – the level of awareness among companies and the importance they ascribe to cybersecurity, is reassuring.

Polling Question 1

How concerned are you with cybercrime?



Others (4%) includes:

We need to learn more before reaching a conclusion (3%)

It's only a minor concern (1%)

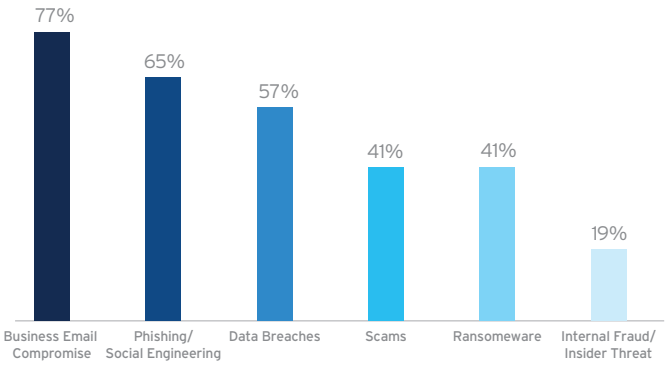
What are the threats — and how are they changing?

Although the cyber threat landscape continually evolves, many of the types of techniques deployed by fraudsters have now been used for many years. For instance, business email compromise (where a criminal attempts to trick someone into transferring funds) is a long-standing favorite of cyber criminals. "What has changed is the scale of the information available on the dark web, which gives criminals a greater ability to deploy such practices," says John Brosnan, Director of Investigations, Citi Security and Investigative Services, North America.

The Citi webinar client poll showed that companies are most worried about business email compromise (77%) and phishing/social engineering (65%)*. Phishing exploits human error to harvest credentials or spread malware, usually via infected email attachments; social engineering is where a criminal impersonates a supplier or executive in order to have funds transferred to their account.

Polling Question 2

What types of cybercrime are your companies most worried about?



*This poll allowed respondents to choose more than one answer.

What is notable about these two top threats is that they 'hack' people rather than technology. Cyber criminals understandably focus on the easiest available target. As companies have invested more in cyber protection, human targets have become relatively more vulnerable and therefore attractive. Activity such as business email compromise and social engineering have become prevalent because of their profitability and the ability of threat actors to cover their tracks. "An individual can send a fictitious email changing invoice instructions, quickly convert it to cryptocurrency and put it into an offline cold storage wallet: it is extremely difficult to trace and investigate such a theft," explains Brosnan. Given its relative anonymity, crypto now plays a major role in cybercrime.

Data breaches, selected by 57% of poll respondents as a key concern, can cause serious reputational damage to companies. One reason for the growing prevalence of data breaches and leakage is increased use of the cloud. However, it is not cloud technology that is most often at fault: about 70% of cases are due to misconfigurations and the failure to implement controls, such as multifactor authentication (MFA) or restrict administration privileges. Companies need to ensure that they design robust controls to manage their data, and implement them in a uniform way regardless of whether they are storing on site, in the cloud, or utilizing a third party.

Ransomware attacks, such as the Colonial pipeline operation, which resulted in disrupted fuel supplies in parts of the U.S. after the firm opted to shut down the system following a cyberattack, were cited as the greatest cybercrime concern by 41% of poll respondents. Average ransom payments have doubled in 2021 — the returns available are prompting more threat actors to use ransomware. Moreover, ransomware is now available as a service on the dark web, lowering costs for criminals and making attacks relatively straightforward to implement. Increasingly, cyber criminals are threatening immediate action if companies engage with law enforcement or employ professional negotiators.

Large companies are obviously an attractive target given the potential rewards on offer. But small and medium-size enterprises — such as healthcare providers — tend to be more vulnerable and are therefore more frequently targeted. Cyber criminals often do reconnaissance that allows them to establish vulnerabilities and companies with inadequate backups and therefore be more willing to pay out when their data is compromised). Similarly, cyber criminals often research companies' cyber insurance (possibly by compromising an insider's credentials), to establish credible ransom demands. Companies need to assess the vulnerability of their applications and, crucially, establish comprehensive training for employees so that they do not click on suspicious links or download questionable files.

Are companies doing enough?

The webinar poll of Citi Commercial Bank clients showed that companies have implemented a range of measures to protect them against fraud and cybercrime, including internal procedures and policies (86%), dual approvals and controls (75%), staff training and education (73%), and segregation of duties (72%). Other options, such as account reconciliation, employee entitlements, and security and verification calls scored less highly.

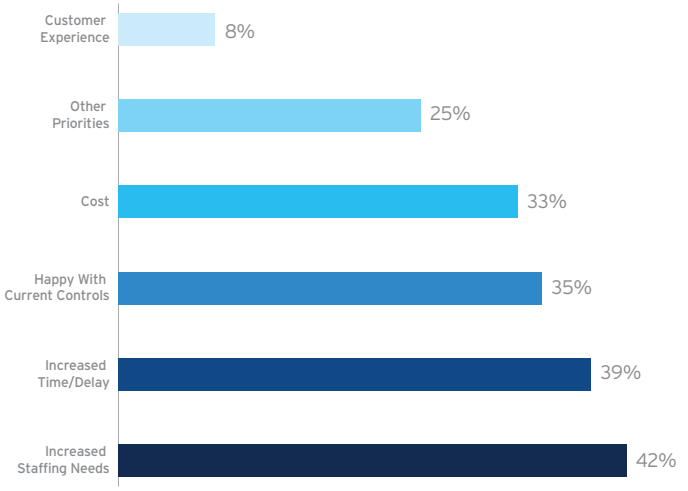
Certainly, internal procedures and policies are crucial in the fight against cybercrime. Dual approval is also critically important; everyone is capable of making a mistake and a quick check by a second pair of eyes can eliminate many errors. Equally, training about risks is essential. People can often intuitively detect when something is right or wrong but without sufficient education, they may not act on the warning signs and threats can be overlooked.

However, it is important to match controls to specific threats. For example, with regards to business email compromise, which is perceived by Citi clients to be the number one risk, the most effective control is a telephone call-back to verify the request. But this was not seen by poll respondents as a priority. Callback verification is quick and straightforward but extremely effective. Despite this, one survey of small and medium-size enterprises in the U.K. showed that five in every 10 businesses did not call back while two in 10 called the (potentially false) number supplied in the email. Just three businesses in 10 bothered to call a known and verified telephone number — sourced independently on the internet, for instance — before authorizing a payee change request.

In the poll, Citi clients said that increased staffing needs (42%) and increased time or delay (39%) were the main reasons why they have not implemented additional controls; other factors such as costs or customer experience were perceived to be of lower importance, while 35% of respondents said they were happy with their current arrangements. "Implementing cybersecurity measures always has to be balanced against internal challenges," says Barron-DiCamillo. "That's why prioritization and partnerships across the organization, between technology and the business for instance, are so important."

Polling Question 3

What has prevented your company from implementing additional controls?



*This poll allowed respondents to choose more than one answer.

New controls can create noise in a company's system without necessarily improving its ability to respond to cyber threats; it is important to ensure that when more sophisticated controls such as threat intelligence data are deployed, processes are put in place to analyze and utilize the information they generate. Equally, companies need to consider whether it could be more efficient, and cost effective, to use a managed service provider rather than doing everything internally.

How Citi is responding to cyber threats

Getting the basics right is a key priority for Citi in order to protect its network and clients. Significant attention is paid to restricting administrator credentials, leveraging Multi-Factor Authentication (MFA), deploying content management tools, ensuring segmentation across networks, imposing restrictions on USBs, and sharing information about internet threats across the organization. Citi also partners with other financial institutions and the wider ecosystem to share information.

Citi has a team of investigators in North America that work around the clock – and coordinate with teams around the world, given the global nature of cybercrime – to identify and eliminate cyber threats to the bank and clients. "In 2020 alone, these investigators were responsible for recovering $100 million in assets for clients," says Brosnan. "At the same time, a key part of the team's role is to educate clients about the nature of the tactics being utilized by criminals."

Citi invests heavily in a wide range of new technology, developing numerous cyber security solutions that leverage artificial intelligence, machine learning and even quantum computing, in its global Innovation Labs and through investments in start-ups via Citi Ventures. Recent innovations include endpoint detection and response, which monitors data in real time and automatically analyzes and responds, and data loss protection solutions.

Another important focus in recent years has been behavioral biometrics software, which not only improves security but can enhance client experience. For many years, Citi has deployed technology that can check whether a client is using their regular device to logon and whether their IP address is familiar.

Key takeaways

- **Develop an appropriate control strategy:** Appropriate controls and capabilities for each of the many cyberthreats faced by companies not only help to avoid risk, but should an attack be successful will ensure that cyber insurance pays out. Education and training about risks and how to respond are especially important as employees are a company's first line of defense; companies also need to encourage a culture where employees know they will be supported when they raise a concern.
- **Planning and preparation are crucial:** If something goes wrong, companies need to know in advance who they should engage with internally and externally, and what information they will need to share with them. It is critical that companies do not find themselves making decisions after an attack.
- **Take a holistic view of costs:** Preparation, planning, controls, training and the many other components of a robust cyber security strategy necessarily requires investment. But a single ransomware attack, for instance, can be devastating to a company financially due to loss of business and reputational risk. In the long-term, prevention is always better than cure.

[1] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

[2] https://www.fbi.gov/news/stories/ic3-logs-6-million-complaints-051721

[3] https://www.jpmorgan.com/content/dam/jpm/commercial-banking/documents/fraud-protection/2021-afp-payments-fraud-and-control-survey-report-highlights.pdf

[4] https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/

[5] https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

*Some polls allowed respondents to choose more than one answer.