Fighting Cybercrime: Citi's Digital Securities Expert Answers Some FAQs

Sabine McIntosh is the global head of Account Services and Digital Security for Citi's Treasury and Trade Solutions business division. Here she responds to some pressing questions about how companies can help protect their treasury systems, information and transactions from cyberthreats.

Where do the biggest threats to cybersecurity come from?

Banks and corporations are accustomed to threats of fraud and theft, having always been prime targets of villains. So, as with any battle, the key to winning the war on cybercrime is to know your enemy.

Most cyberthreats result from intrusive activity, and that activity can come from either inside or outside an organisation.

Fortunately, insider attacks are less common than outsider attacks. Unfortunately, however, they also are harder to detect. Internal attacks are generally initiated by individuals with access to security or transaction systems, people whose malice can include activities such as redirecting funds or sharing confidential information. It is not unusual for these employees to go undetected because they are trusted and valued.

Outsider attacks, on the other hand, can come from many types of intruders. For example, "hacktivists" are primarily motivated by political agendas rather than monetary gain. They typically rally support via social media forums and provide their supporters with tools to attack a particular target. Their tactics may also include increased attention in the press, which means victims can suffer loss of public trust besides operational or financial consequences.

Cyberterrorists, another brand of modern-day bad guys, can include money launderers and one of the most sinister criminal groups of all: state-affiliated terrorists, who usually act on behalf of a hostile country seeking to undermine the digital integrity of another. These attackers may invade a system and lie dormant for years, sometimes tracking information during that time, before they suddenly assault or disable a system.

Internet-based social networking sites and social engineering have become popular platforms for cybercriminals to identify like-minded miscreants and engineer attacks. In fact, spear phishing, baiting, from-a-friend communications and similar social engineering schemes are among the most prevalent threats facing organisations today. These attackers secure access to restricted information by exploiting psychology.

Masquerading, for example, is a technique commonly used by fraudsters to acquire personal information and gain access to financial accounts. Spear-phising attacks can compromise an individual's personal information and create vulnerabilities for others. If, for instance, an executive opens an email from a spear phisher that looks like it's coming from a trusted source, the spear-phishing crook could compromise the executive's email account and then pose as the executive and send an urgent email to an employee asking for confidential information or to authorise a transaction. Employees usually comply. In some instances, employees actually bypass security requirements to expedite the request since they know it is coming from an executive they know.

How can my organisation fend off cyberattacks?

Understanding the sources of threats is the first step to mitigating security breaches.

Robust cybersecurity systems and operating processes are critical. However, a large part of preserving network and transaction security involves good old common sense.

Take insider threats, one of the most basic things that companies and their banks must do is to maintain up-to-date records of employees who are authorised to access banking systems and transactions. This includes a strong focus on the credentials, such as security tokens, for accessing systems and applications and the levels of entitlement. When personnel changes occur, records and security access must be immediately updated.

Employing multiple levels of approval for transactions, particularly high-value transactions, also increases controls and helps reduce the risk of villainous inside activity. Citi's CitiDirect BE® online corporate banking platform, for instance, supports up to nine levels of approval for releasing payments. In addition, transactions themselves need to be monitored. Using reporting tools that help spot unusual transactions and account activity are invaluable. With many cybercrooks gaining access to corporate networks and information via social engineering tricks, employees need to be trained on how to handle requests from anyone contacting them claiming to represent a bank or asking for sensitive information. Regular communication and training help reinforce the need to be on the lookout for fraudsters and make employees aware of the latest threats.

Cybersecurity also requires discipline and vigilance in using antivirus software and in updating systems and browsers. Using an unprotected device, even once, opens the door for a cyberoutlaw to wreak havoc. So discipline, in this sense, means ensuring that personal gadgets that employees use to log in to corporate networks, in addition to office PCs and laptops, are loaded with the most up-to-date virus and malware protections.

What protection does Citi provide against cyberthreats?

Financial institutions like Citi have invested huge amounts of money and resources into creating cyberforts that aim to protect their network and data.

Some of the weapons in Citi's security arsenal are visible to customers. Others work in the background and only make themselves known when there are signs of a potential breach or threat.

Citi's cybersecurity strategy includes, for example, a multilayer model of defence for spotting and curtailing invasions. It involves tagging information to detect suspicious activity at the earliest stages, which is when an attacker is trying to find a vulnerable spot in a system. Tagged information is used to identify and thwart specific incidents and also to spot future threats.

Over many years, Citi has developed a three-pronged approach to digital security that includes channel protection, transaction monitoring and data privacy.

Channel protection involves blocking attackers from entering an online platform or data transmissions channel, for example. This control is achieved through strong login credentials for authentication. All data that is exchanged with our clients is protected with robust encryption tools that prohibit attackers from reading information while it is being transferred between clients' systems and Citi.

Many attackers are focused on transactions themselves so both companies and their bank need to be vigilant about monitoring payments – the second prong – to detect any outliers. Citi's Innovation Labs are exploring solutions that aggregate a company's payment data across countries, currencies, payment methods and beneficiaries to derive normal payment patterns and then flag transactions that fall outside historic trends for review.

The third prong involves protecting data privacy. This is achieved though the bank's data privacy and governance policies and a focus on entitlements and ensuring that only authorised persons can view and access information. Data privacy also is protected through multiple levels of security, backing up data at different sites, and using a variety of systems to protect and ensure the accuracy and reliability of data.

What if a cyberattack happens?

As is the case with any crime, acting quickly when a cybercrime hits is essential. So is communicating that the crime has occurred. Gone are the days of a hush-hush attitude towards cyberattacks. Given the high stakes involved, financial institutions and their clients must work together and communicate immediately when a breach does occur.

One reason is that the sooner all relevant parties and authorities are aware of cyberintrusion, the more likely it is that the culprit will be caught and that any stolen funds recovered.

Corporations and their banking partners must remain united in their efforts to curtail cybercrime. Sharing information, new ideas and best practices among them makes both parties even stronger.

Treasury and Trade Solutions
transactionservices.citi.com

GRA26733 04/2016