Cybersecurity: the impact to the financial supply chain

It's no longer enough for corporates and banks to simply react to cybersecurity risks – they must be proactive and anticipate what adversaries will do next.

Treasury and Trade Solutions

citi

Raj Shenoy
Global Head, Digital Security, Treasury and Trade Solutions, Citi

Cybercrime, an attempt to access or damage a computer network or system to steal data or money, costs the global economy an estimated USD445 billion worldwide every year in direct damage and recovery costs. The number of cyberattacks is growing as companies digitize and the number of connections to the internet grows. By 2020, there will be an estimated 50 billion internet connections compared to 15 billion currently: each is a potential risk.

The gap is widening between criminals' ability to attack and corporates' and governments' ability to defend themselves: it takes an average of 265 days to discover a network breach. To close this gap, Citi shares information that may be red flags of potential breaches with clients, other banks, and regulators, helping to prevent attacks to their own systems in the future. By partnering together, participants will make the financial ecosystem stronger.

Understanding the motivation of attackers

To develop an effective security strategy, it is necessary to understand who attacks corporates, how they do it, and why. There are five cyberthreat actors – nation-states, cybercrime, terrorism, hacktivism, and insiders – each with different targets, methods, and objectives.

Nation-state actors aim to steal intellectual property and engage in intelligence collection to advance national interests. They are difficult to defend against because of their potentially significant resources and advanced capabilities.

Cybercrime actors are mainly motivated by financial gain, but can cause damage when monetization attempts fail. Their typical methods include spear phishing and similar social engineering techniques, automated crime tools, fraud, botnet-enabled distributed denial-of-service attacks, and cyberextortion or ransomware.

Terrorist actors are politically or ideologically motivated and aim to instill fear. Typical methods are destructive cyberattacks, designed

to destroy, degrade, disrupt, or deny system operation, and cyber-enabled functions to recruit, incite, train, plan, and finance operations.

Hacktivists generally seek publicity to further their geopolitical or social agenda and usually operate disruptive campaigns primarily via distributed denial-of-service attacks and website defacements.

Insiders are potentially the greatest threat to corporations. They may seek financial gain or wish to cause harm for a perceived wrong. Corporates need to adopt a different strategy to detect and defeat insiders given their inside knowledge, which can more easily enable them to steal data, conduct fraud, or cause damage undetected.

Defeating this wide range of attackers, who use a huge and evolving range of methods, is challenging: corporates have to get it right 100% of the time, whereas criminals only need to get it right once. However, in reality, corporates have multiple opportunities to successfully prevent or defeat attacks: the reconnaissance phase, the initial compromise, the establishment of a foothold, the ability to escalate privileges, and the ability to exfiltrate data. Attackers must go through each phase for a successful attack. That gives corporates or banks the ability to customize defenses for each stage, depending on the type of actor.

Business, both externally and internally, is increasingly dependent on electronic interaction and communications across a broad spectrum of partners inside and outside the company.

At Citi, this customization of defenses occurs at Citi Security Operations Centers (SOCs), which house teams that constantly monitor for intrusions and which collect data on patterns of activity (such as unsuccessful defensive measures so that lessons can be learned). Citi Cybersecurity Fusion Centers (CSFCs) comprise multiple cybersecurity teams from across Citi to better attribute the threats, see if such threats are affecting other organizations, and determine what lessons Citi might learn from them. The overall goal is to stop the adversary at the reconnaissance phase before they can actually conduct their cyberattacks.

The impact on treasury

Attacks on the treasury can take a number of forms. One of the most common is treasurer impersonation, which involves a combination of technology and social engineering. For example, a treasurer may update their social network account with an event they will be speaking at. A hacker uses that site as an entry point and gains access via an online brute-force attack to guess the treasurer's login ID and password.

The hacker follows up by making connections with the treasurer's associates (such as key suppliers or employees) linked to that account before sending a social networking site message to all associates asking them, for example, to click on a link to the upcoming conference at which the treasurer is speaking. These users are then compromised by malware when they click on the link. The malware infection enables the hacker to compromise the credentials of the contacted parties' email accounts and send directions to the treasurer's account payable

colleague to change vendor bank details and transfer funds. Similar attacks may use a telephone call to request a payment (often claiming that, for business reasons, such as an M&A or regulations, the details of the request must be kept secret).

The impact on the financial supply chain

Business, both externally and internally, is increasingly dependent on electronic interaction and communications across a broad spectrum of partners inside and outside the company. For example, treasury interacts externally with its banks, vendors that may be performing outsourcing functions, and suppliers; and internally with functions such as technology or human resources. It is critical to ensure that end-to-end security is in place across all of these interactions.

Key controls to safeguard the company include but are not limited to:

- **Data protection:** information, including customers' or suppliers' details, is as great a target for criminals as transactions, as it can be easily monetized.
- **Third-party information-security assessment:** all vendors must have appropriate controls. Regular questionnaires, reviews, and audits are helpful to access new partners' security measures.
- **Security incident management:** corporates need to have procedures so people know what to do if security is breached.
- **Vulnerability assessment:** controls should be tested periodically, ideally by a third party, using tools similar to those used by hackers.
- **Global ID administration:** there must be a prompt method to update, modify, or delete access to systems as employees' roles change to avoid vulnerabilities.
- **Privileged user-managed access:** entitlements to sensitive internal and external systems and networks must be appropriate for each employee.
- **Data:** reports can be used to monitor and identify potential problems as early as possible to trigger security incident-management processes. Alternatively, data can be mined to identify trends and best practices relating to user access, for example.

Security best practices

Improving internal fraud prevention and the reaction to such on discovery depends on prevention and post-attack mitigation within the financial center.

Prevention can be split into three areas, each of which has distinct best practices that enhance security. Internal controls include implementing electronic payments for recurring check disbursements, using additional levels of control for new payee authentication, and minimizing spare check stock and maintaining tight control over inventory. In addition, surprise audits should be conducted and exception items and account activity should be reviewed on a daily basis.

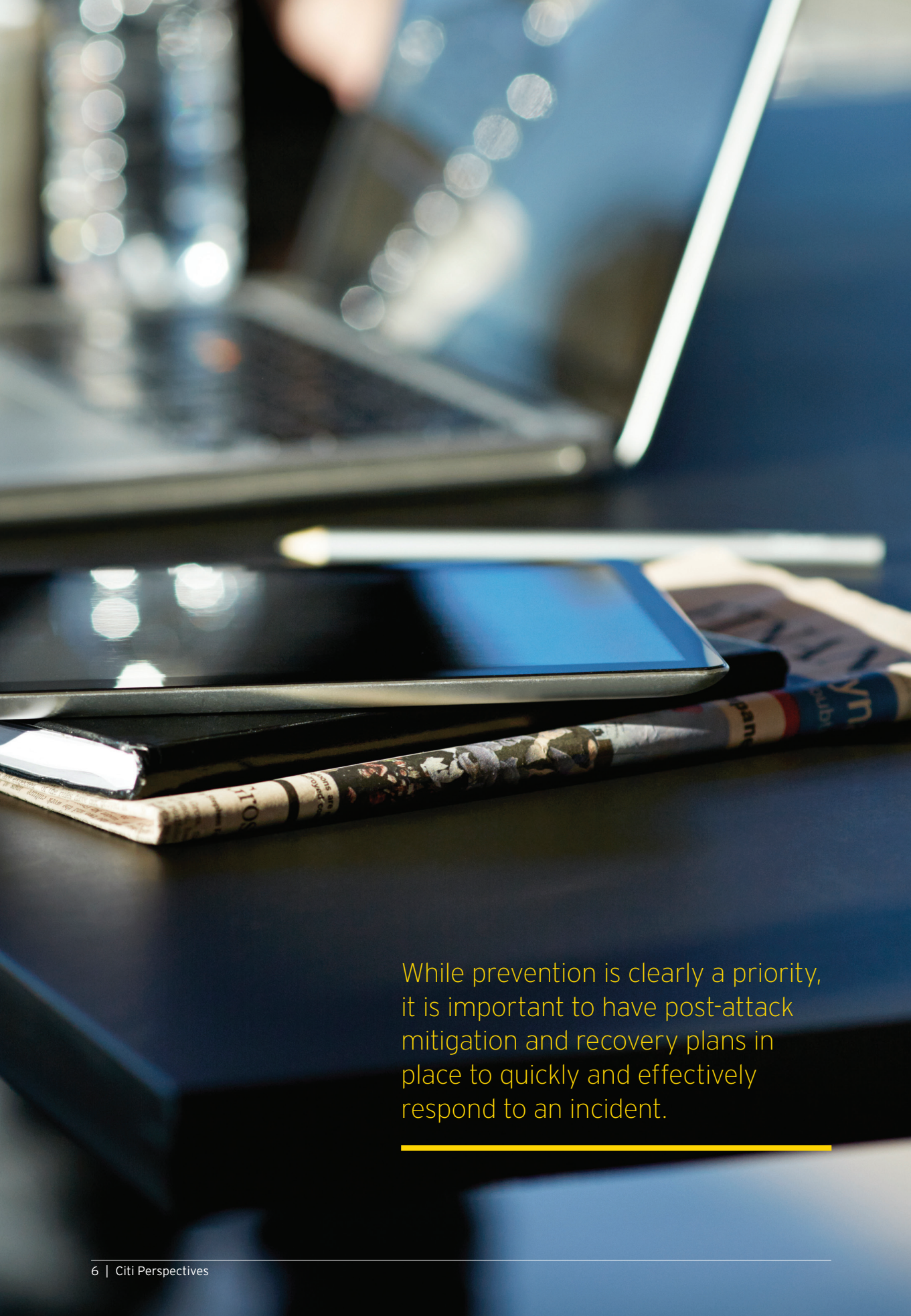
Staff must be thoroughly screened and then trained on cyberthreats and potential fraud.

Transaction controls are one of the most important security areas for corporates. Robust controls should be in place for access to systems and data, and locked beneficiary templates (preformats) should be used for payments to help prevent unauthorized changes. Citi also recommends the use of separate deposit and disbursement accounts to allow depository accounts to block all check presentment.

Human resources risk mitigation is also essential. Staff must be thoroughly screened and then trained on cyberthreats and potential fraud. Those in financially sensitive assignments must be periodically rotated or have mandatory absence periods so there is no single point of potential failure and threats are mitigated. Maker-checker segregation of responsibilities should be enforced, and this should be supported in system workflows.

While prevention is clearly a priority, it is important to have post-attack mitigation and recovery plans in place to quickly and effectively respond to an incident. These include the issuing of alerts and reminders so staff know what to do in the event of an actual or potential compromise. It should also be clear whom to contact at the bank should suspicious activity occur.

Furthermore, a playbook on how to manage a security incident should be in place with practice drills to insure readiness. The faster an action is taken, the more likely it is that funds will be recovered or damage prevented.



While prevention is clearly a priority, it is important to have post-attack mitigation and recovery plans in place to quickly and effectively respond to an incident.

Treasury and Trade Solutions
transactionservices.citi.com

© 2018 Citibank, N.A. All rights reserved. Citi and Arc Design, CitiConnect and CitiDirect are trademarks and service marks of Citigroup Inc. or its affiliates, used and registered throughout the world. The information and materials contained in these pages, and the terms, conditions, and descriptions that appear, are subject to change. The information contained in these pages is not intended as legal or tax advice and we advise our readers to contact their own advisers. Not all products and services are available in all geographic areas. Your eligibility for particular products and services is subject to final determination by Citi and/or its affiliates. Any unauthorized use, duplication or disclosure is prohibited by law and may result in prosecution. Citibank, N.A. is incorporated with limited liability under the National Bank Act of the U.S.A. and has its head office at 399 Park Avenue, New York, NY 10043, U.S.A. Citibank, N.A. London branch is registered in the UK at Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB, under No. BR001018, and is authorized and regulated by the Financial Services Authority. VAT No. GB 429 6256 29. Ultimately owned by Citi Inc., New York, U.S.A.

These materials are provided for educational and illustrative purposes only and not as a solicitation by Citi for any particular product or service. Furthermore, although the information contained herein is believed to be reliable, it does not constitute legal, investment or accounting advice and Citi makes no representation or warranty as to the accuracy or completeness of any information contained herein or otherwise provided by it.

GRA29662 07/18