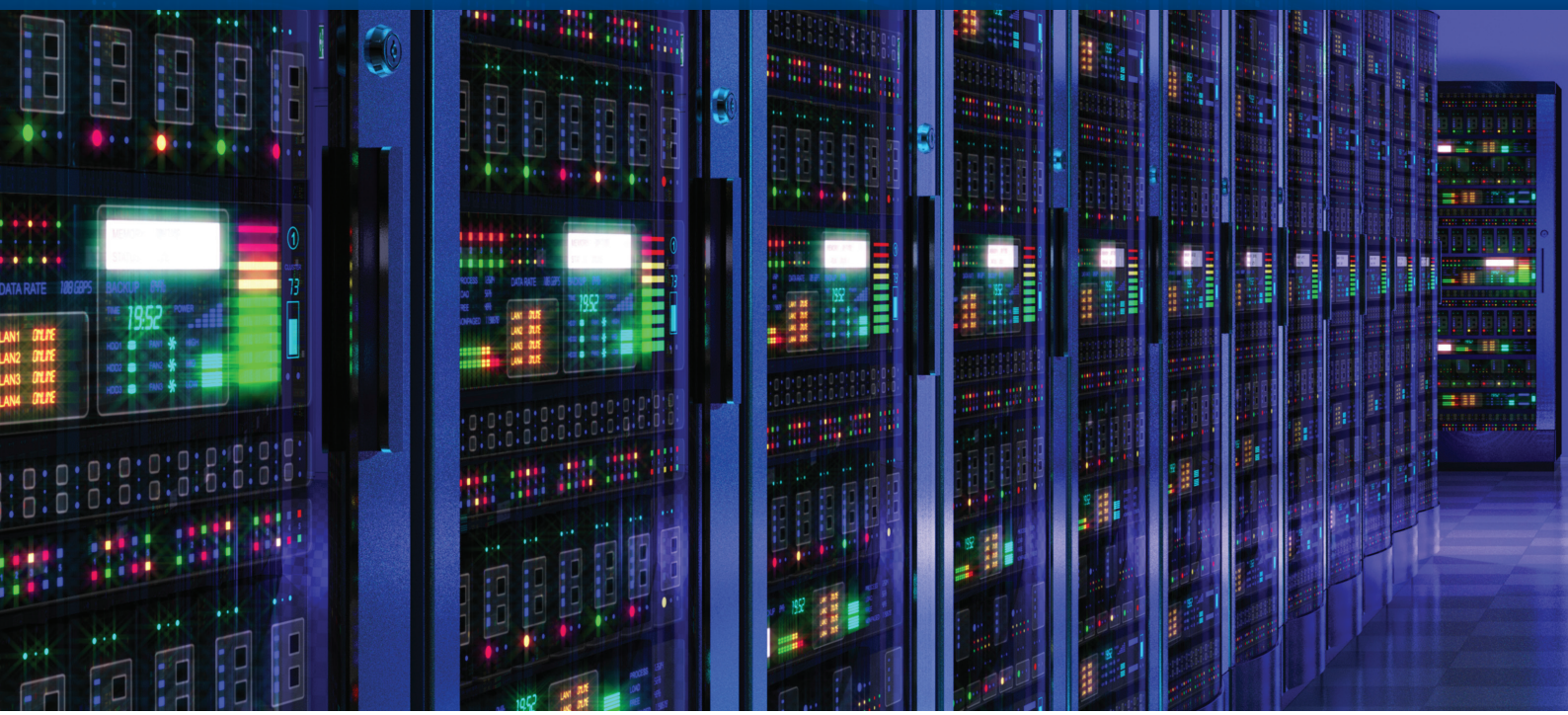


INNOVATION SPOTLIGHT

Innovation: a major weapon in the fight against cyber demons

Innovation, information and cooperation fortify the defense against cybercriminals.

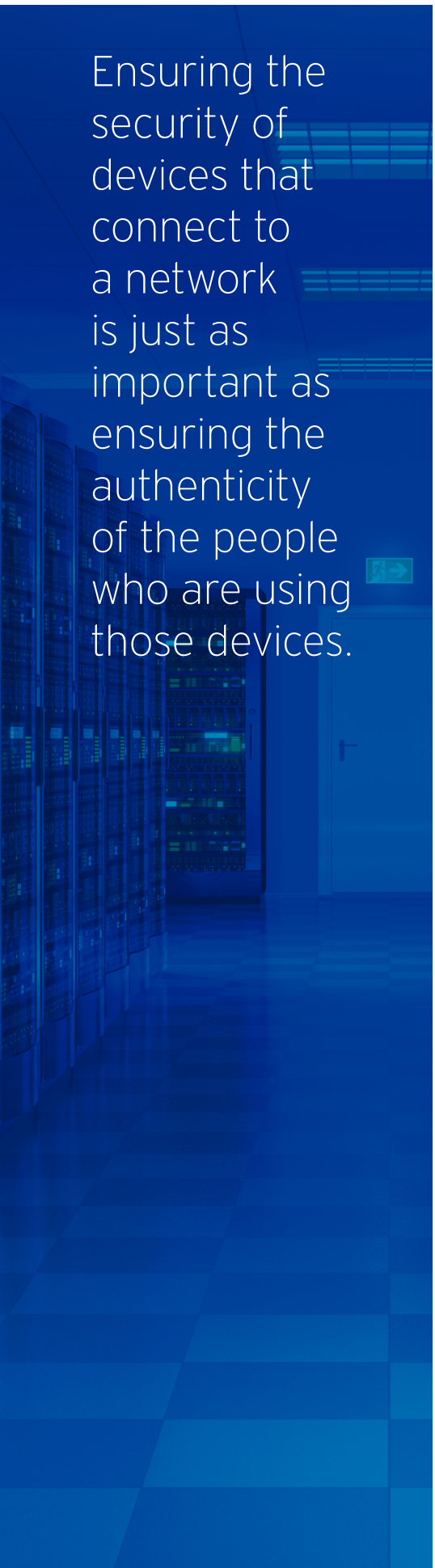
Rajesh Shenoy
Global Product Manager, Digital Security, Treasury and Trade Solutions, Citi

Banks and businesses have always been the targets of robbers, cheats and fraudsters. The days of stage coach heists, however, are long gone. Even currency-loaded cash registers and vaults that have lured evil doers for centuries could become a thing of the past as consumers and businesses migrate to non-cash payments.

Today, the thieves and attackers are finding digitization to be more convenient. They are increasingly wreaking financial havoc in the cyber world, not the physical world. In fact, cybercrimes have quickly become one of the world's most prevalent crimes. According to a study by Juniper Research, the cost of cybercrime to the global economy will be $2.1 trillion dollars by 2019.

In the U.S., concerns about the prevalence of cybercrimes led to the formation of the Cyber Threat Intelligence Integration Center to ramp up government agencies' defenses against cyberattacks.

Similarly, governments and businesses around the globe have waged an all-out war against cybercriminals. Banks have ramped up their battlefield strategy with technology-based innovations that strengthen not only their ability, but their customers' ability, to help detect and head off nefarious cyber activity.



A monster with many tentacles

Cyberthreats emanate from a multitude of sources inside and outside an organization, and their tentacles can be far-reaching. Take the massive hack of a prominent multinational electronics and media conglomerate's computer network. In another high-profile case, a cyber-hacker managed to transfer millions of dollars from a corporate bank account. Operational and security weaknesses can have a huge impact on supply chains and financial accounts.

With so many mission-critical financial activities being automated and digitized, cyber-security is clearly a top priority among corporations and the financial institutions with whom they interact and interconnect.

Partnerships between banks and their clients are critical for end-to-end security. Criminals look for opportunities to exploit weak links and often re-use successful attack methods from one victim to another. Aligning closely and sharing information on threats and security best practices can reduce vulnerabilities, helping to protect all partners and their assets.

Battling the enemy

In any battle, one of the best offenses is a good defense. Prevention, detection and rapid response to digital security attacks extend beyond technology to encompass people and processes. That's why financial institutions have invested huge amounts of money and resources to create "cyber-forts" with multiple layers of protection for their networks and the data that flows through them. Some of the weapons in banks' security arsenals are visible to their clients. Others are invisible, working in the background and only making themselves known when there are signs of a breach or a threat.

Still other innovations in the ongoing war against cybertheft and fraud have yet to be deployed. Emerging technologies are continually being analyzed, developed and tested in R&D centers such as Citi's Innovation Labs to ensure that they meet robust security and regulatory requirements and also to improve clients' experiences accessing and using electronic banking services.

Biometric authentications

Biometrics technologies that analyze unique physical or behavioral characteristics, for example, offer possibilities to both streamline user authentication and link identity verification to an actual person rather than something they must remember or carry with them.

The biometric tools that Citi's labs continue to monitor and test include physical characteristics such as voice, face, iris and finger print technologies. Specialized software uses customers' unique natural characteristics to verify their identities. These evolving technologies are expected to provide customers with convenient alternatives to token-based security that relies on PINs, passwords and challenge questions. As promising as these technologies are, however, banks need to ensure that they meet the highest hurdles of security before rolling them out to customers. Furthermore, protection of biometric data becomes critical since it is easier to reset a password than it is to change a person's biometrics.

Bank technologists also are assessing biometric technologies that can function as passive login tools. These technologies use behavior patterns such as typing rhythms and patterns in mouse movements that are unique to individuals to determine if the person using an application is the person they say they are — and to block impersonators.

Device security

Ensuring the security of devices that connect to a network is just as important as ensuring the authenticity of the people who are using those devices.

The reality is that most cybersecurity comes down to discipline and vigilance on the part of IT departments and individual end users. Using antivirus software and updating browsers and systems should be regular preventive measures that extend to the personal computers and mobile devices that employees use to access company platforms or execute transactions. Unfortunately, too many users have learned the hard way that using an unprotected device, even once, can open the door to cybercriminals.

Even so, not all companies and their employees are as diligent as they could be about ensuring that the latest virus and malware protections are in place. Banks are becoming aware of the device security gaps among their client base and are ramping up their defenses to include a new generation of device identification and malware detection tools. These software programs sit on the bank's internal network and provide integrity checks of external devices connecting to the bank, looking for signs of malicious modification or infection.

Evolving device security technologies and cyber-intelligence gathering by banks allow for monitoring of information where customers' private credentials are being publicly distributed by cybercriminals who have performed a data breach.

PREVENTION, DETECTION, AND RAPID RESPONSE TO DIGITAL SECURITY ATTACKS EXTEND BEYOND TECHNOLOGY TO ENCOMPASS PEOPLE AND PROCESSES.

In the past, some financial institutions and corporations may have taken a "hush-hush" attitude to cyberattacks.

Out-of-band security

Cyber robbers are predominantly focused on transactions themselves and diverting funds their way. Thus, transaction security is another major pillar of defense. A strong focus on entitlements, including keeping entitlement records up-to-date and using multiple levels of authorization, are all common sense measures for ensuring that the correct person is initiating and executing transactions and for mitigating the chances of a rogue employee corrupting transaction processes.

Having a diverse set of people and processes involved in high-value transactions increases control and can reduce the chance of fraud. Toward this end, out-of-band authentications are another way that banks are investigating an additional layer of security at the transaction level.

Out-of-band interactions involve using a device separate from the primary banking channel to require an additional level of transaction approval or confirmation. In a low-tech example of out-of-band security, when a credit card company issues a new card to a cardholder by mail, the cardholder must phone an 800 number to activate it. In a higher tech example for a corporate banking transaction, a high-value payment or funds transfer initiated online could be authenticated via a one-time password sent to, or a call made to, the initiator's mobile device to provide an extra level of security.

The nearly ubiquitous use of mobile devices among business managers has fostered new models for digital security and also opportunities to make electronic banking more convenient. Citi, for example, has rolled out with corporate online banking customers a mobile app version of hardware security tokens that simplifies the login process for its CitiDirect BE online banking platform. The new smartphone token application can eliminate the need for users to carry separate hardware tokens to securely log into the banking platform. Instead, they can use the app on their smart devices to generate dynamic passwords and link to CitiDirect BE. Citi also is piloting the use of one-time SMS and voice codes as an alternative to hardware tokens for logging on to mobile and tablet versions of CitiDirect BE for viewing balances and authorizing banking transactions.

Mitigating payment risks via analytics

Technologists also are pursuing the use of data analytic tools to identify unusual payment transactions, which might include potentially fraudulent payment transactions. Leveraging large volumes of payment data across countries, currencies, payment methods, beneficiaries, etc. creates a baseline of normal patterns of payment activity. Using this data, Citi's data scientists are exploring statistical models to monitor transactions and alert clients when transactions fall outside of historical trends. If, for instance, there is a change in pattern for recurring payments to a beneficiary, or payments are made to a country where they are not normally made, or payments are authorized by someone other than the normal authorizer, flags can be raised.

A shared crusade

The mission is to prevent, detect and respond to fraud and data theft. Continuous "smart experiments" by Citi's Innovation Labs to evaluate and develop new solutions leveraging emerging technologies provides Citi with a pipeline of new capabilities to stay ahead of emerging and evolving threats.

In the past, some financial institutions and corporations may have taken a "hush-hush" attitude to cyberattacks. No more. Given the high stakes involved, financial institutions and their clients must work together and communicate quickly and efficiently when a breach does occur. One reason is that the sooner all relevant parties and authorities are aware of a cyber intrusion, the more likely it is that the culprit can be caught and that any stolen funds can be recovered.

Security is about more than protecting systems and resources — it's about providing the peace of mind that allows companies to operate without fear. Innovation and collaboration are priceless weapons for elevating attacks on cybercrime to maximum strength. Corporations, banking providers, technology companies and government agencies — domestically and globally — must remain united in their efforts and perched at the forefront of new security options and innovations. Sharing information, new ideas, methods and best practices among all parties makes every party stronger. ■

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions

1564155 05/17