SPECIAL REPORT: CYBERSECURITY

TREASURY & RISK

THE FUTURE OF FINANCE TODAY

Cybersecurity: Protective Measures Treasuries Should Be Taking

PAGE 2

Sponsored by Citi and Kyriba

Cybersecurity: Protective Measures Treasuries Should Be Taking

BY RUSS BANHAM

Payments fraud remains a thorn in most corporate treasurers' sides, but several best practices can shore up corporate defenses.

Much has changed since the early 20th century bank robber Willie Sutton, when asked why he chose his targets, reportedly said, "Because that's where the money is." Criminals are now using tools Sutton couldn't have dreamed of, but their philosophy in choosing targets remains pretty true to his.

Many attacks are now perpetrated online, with alarming growth in volume and sophistication over the past two years. Equally distressing is the range of perpetrators, from conventional hackers and disgruntled employees to well-funded nation-states, terrorist organizations, and criminal groups. Their top target in many attacks: corporate treasury.

"Cybercriminals consider corporate treasury—due to its mission-critical function of managing the flow of funds—to be a high-value target."

—RAJESH SHENOY
GLOBAL HEAD OF DIGITAL SECURITY, TREASURY AND TRADE SOLUTIONS, CITI

That's where the corporate money is. But some hackers that target treasury have more in their sights than direct theft of company funds. Treasury systems are repositories of sensitive data that can be stolen. Crucial financial systems also can be shut down, either for ransom or to promote a geopolitical agenda. Aside from the financial costs of these disruptions, companies confront the risk of serious reputational damage, which may have a lingering business impact.

While many corporate treasuries have thoughtful measures in place to ward off known forms of malware, it's tomorrow's (currently unknown) malware that gives deep pause for information security experts. Hackers and fraudsters are in the business of inventing new types of ever-more-innovative cyberattacks, their methods continually evolving to achieve specific aims.

In this work, corporate treasury is in the crosshairs. "Cybercriminals consider corporate treasury—due to its mission-critical function of managing the flow of funds—to be a high-value target," says Rajesh Shenoy, global head of Digital Security, Treasury and Trade Solutions at Citi. "Consequently, treasuries must do all they can to make their operations less of a target by hardening their systems, processes, and procedures to be less susceptible to a cyber event taking place."

Payments Fraud Continues to Grow

Payments fraud is a key cyber event that treasuries need to protect against. According to the 2018 Payments Fraud Survey of nearly 700 treasury and finance professionals conducted by the Association for Financial Professionals (AFP), a record 78 percent of treasury organizations were hit with payments fraud in 2017.

"It is alarming that the rate of payments fraud has reached a record high despite repeated warnings," says Jim Kaitz, AFP's president and CEO. "In addition to being extremely vigilant, treasury and finance professionals will need to anticipate [such] scams and be prepared to deter these attacks."

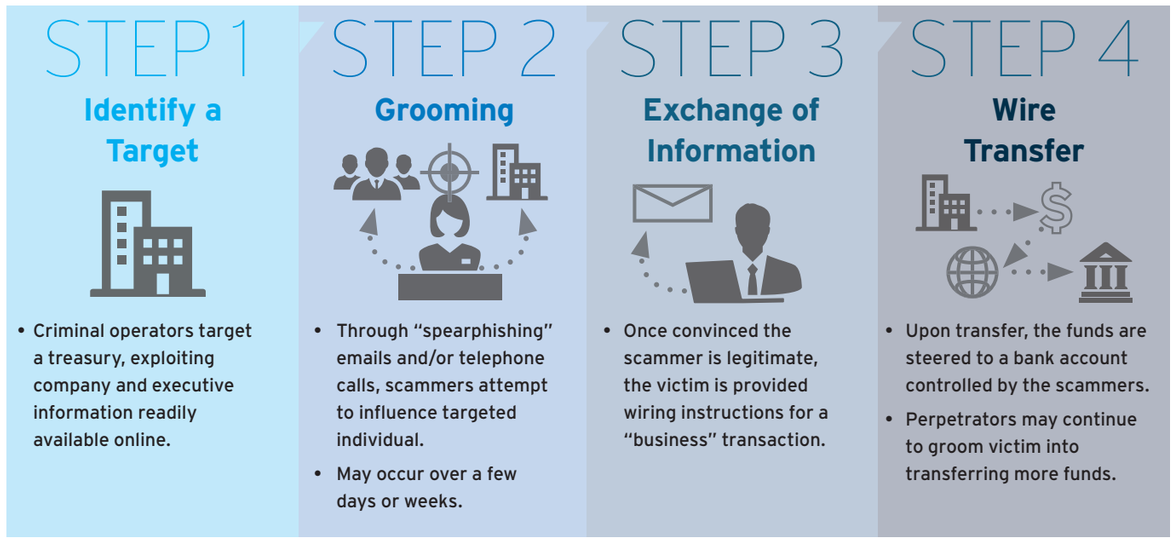
A key method of perpetrating payments fraud is business email compromise, whereby an attacker gains access to a corporate email account and spoofs the owner's identity to defraud the company—or its employees, customers, or partners—of money.

Business email compromise scams are among the top fraud threats to corporate treasury and finance, with both the frequency of attempts and the total dollar amounts stolen increasing in recent months—dramatically in some cases. The AFP survey indicates that 77 percent of organizations experienced at least one such attack in 2017. More than half the scams (54 percent) targeted wire payments, followed by checks at 34 percent. A typical ruse involves persuading an employee to send a fraudulent invoice for processing by accounts payable, which unknowingly makes the payment to a bank account controlled by the fraudster.

Shenoy agrees with these findings. "Increasingly, a combination of technology and human elements looking to

(continued on page 6)

Anatomy of a Business Email Compromise Scam



Source: FBI

Kyriba Recognized as a Global Leader

When technology analyst firm IDC completed its latest vendor assessment of SaaS and cloud-enabled treasury and risk management applications, one vendor rose to the top.

Innovation, Security and Customer Commitment

IDC positioned Kyriba along with other global vendors based on criteria covering customer satisfaction, depth of functionality, data security, SaaS architecture and more.

Kyriba's enterprise cloud platform enables forward-thinking teams at nearly 2,000 companies worldwide to improve key capabilities for cash and risk management, payments and working capital optimization.

To learn more and get a free copy of IDC's latest MarketScape, visit www.kyriba.com or call 1-855-KYRIBA-0.

kyriba

www.kyriba.com
1-855-KYRIBA-0

Kyriba

kyriba

Kyriba empowers forward-thinking treasury and finance teams to optimize key capabilities for cash and risk management, payments and working capital strategies. Kyriba delivers a highly secure, 100% SaaS platform, superior bank connectivity and a seamlessly integrated solution set designed for tackling many of today's most complex financial challenges. Thousands of companies worldwide rely on Kyriba to streamline key processes, enhance fraud protection and compliance, and accelerate growth opportunities through improved decision support. IDC, a global technology analyst firm, recently recognized Kyriba as the category leader for worldwide SaaS and cloud-enabled risk management applications. For more information, visit www.kyriba.com.

PRODUCTS AND SERVICES

Treasury Management

Kyriba's award-winning treasury management capabilities include cash positioning, cash forecasting, advanced forecasting, variance analysis, liquidity forecasting, in-house banking, and multi-lateral netting. Clients also benefit from full accounting, GL posting, and bank-to-book reconciliation workflows. The cash and liquidity modules are supported by Kyriba's financial data and connectivity hub.

Payment Management

Kyriba's comprehensive payment solution helps clients initiate, approve and release payments to any of their banks globally. Kyriba also supports payment factories, including multiple routing options to integrate all corporate payment workflows in a centralized hub. Kyriba's advanced security options – including real-time payments fraud detection – ensures that payment workflows are standardized, secured and monitored.

Working Capital

Kyriba's working capital solutions enable clients to support the working capital needs of their supply chain through the use of two early payment programs, dynamic discounting and reverse factoring. Kyriba's ability to combine cash management, payments and supplier financing in a single platform uniquely positions Kyriba as the leader in working capital technology solutions.

Risk Management

Kyriba supports a wide array of risk management requirements for treasurers and CFOs, including financial, regulatory and operational risk. Kyriba's financial risk module delivers exposure management, position keeping, valuations, accounting and hedge accounting across foreign exchange, interest rate and commodity asset classes. Kyriba helps manage liquidity risk by fully supporting investments, borrowing and intercompany transaction workflows. Kyriba's embedded market data and trade portal architecture offers complete integration for straight-through processing and workflow automation.

Control and Compliance

Kyriba enables financial executives to implement strong financial controls, sophisticated audit reporting, and industry-first capabilities for real-time fraud prevention. To strengthen operational security and align with an organization's information security policies, Kyriba also offers a comprehensive array of advanced security features, including two-factor authentication, IP filtering and enterprise single sign-on.

Business Continuity

Kyriba's SaaS (software as a service) platform offers the comfort of SOC1 and SOC2 compliance. Kyriba provides a fully redundant architecture to ensure that Kyriba is always operational and accessible. Kyriba ensures the entire solution is replicated and available – data, reports, bank connections, ERP interfaces, security protocols, login procedures, and even the same web site. Kyriba commits to industry best uptime and RTO/RPO metrics, so clients know that Kyriba is always available.

CONTACT INFORMATION

KYRIBA

Kyriba 9620 Towne Centre Drive
Suite 250
San Diego, CA 92121

Tel:
+1 858 210 3560
+1 855 KYRIBA 0
E-mail: treasury@kyriba.com
Website: www.kyriba.com
Twitter: @kyribacorp

CYBERSECURITY (cont'd from page 3)

compromise people, manipulating them to take specific actions for what they believe are authentic business purposes," he says. "Most people think they would spot such charades, but the truth is they are extremely well thought out and crafted."

Data Breaches a Major Concern

Although business email compromises make up the bulk of payments fraud schemes, other treasury-focused cyberattacks are predicated on stealing valuable data—typically including the names, addresses, bank account information, and bank statement details of vendors, partnering organizations, employees, customers, and other payers and payees. Once they've stolen personal data, cyber thieves hold it for ransom or sell it directly on the murky underground forums populating the dark web.

According to Dark Web News, bank accounts hold more value than other forms of identity in that world. A $2,000 account balance, for instance, could sell for about a tenth of its value, or $200. Multiply this figure by hundreds or thousands of accounts, and the incentive for identity theft increases exponentially.

Corporate treasuries that suffer a successful attack resulting in a breach of personal data can incur stiff penalties. The new General Data Protection Regulation (GDPR) in the European Union, for example, imposes substantial fines on companies for noncompliance—up to 20 million euros or 4 percent of global annual turnover, whichever is higher. All companies that do business in the EU must comply with the regulation.

> "In an organization of 25,000 people you might have 10 or 15 people within treasury, narrowing a hacker's ability to perpetrate a phishing attack. At the same time, though, this makes it easier to seek out the most vulnerable target."
>
> —BOB STARK
> VICE PRESIDENT OF STRATEGY, KYRIBA

Other cyberattacks, like ransomware, involve encrypting a treasury system to curtail its service until a ransom is paid. And paying the money doesn't guarantee the company's desired outcome. "In Eastern Europe, many organizations paid the ransom to have their systems decrypted and unlocked, but in some cases they nonetheless remained locked," says Shenoy.

He's referring to malware called NotPetya, which was blamed for disrupting business operations at shipping ports, advertising agencies, law firms, and retail outlets in 2017. Once inside these organizations' networks, the malware destroyed the infected machines' file systems. The goal was not financial gain; rather, it was geopolitically motivated, designed to completely shut down corporate networks for purely malicious reasons.

The attacks were followed by the similar Bad Rabbit malware that infected the networks and systems of several news media organizations in Russia, Ukraine, and Turkey. Hackers demanded payment in bitcoin to decrypt the files they had encrypted, then neglected to make good on some of their promises. The malware was eventually decrypted when keys to unlock it were provided by Internet security firms.

Hacker Sophistication Requires Employee Vigilance

How often do cyberattacks hit corporate treasuries? It depends. "For the most part, treasuries are attacked on an infrequent basis, but in some large organizations, these attempts are fairly common, as many as multiple times a day," says Bob Stark, vice president of strategy at Kyriba, a provider of cloud-based treasury management software systems. "A small company, on the other hand, might be attacked once or twice a year."

There are no current statistics on the aggregate number of successful cyberattacks against corporate treasuries or the total cost of these crimes. For security purposes, many treasuries prefer to stay tight-lipped on the subject. However, the interviewees agree that the risk and financial impact are substantial. Based on anecdotal evidence, losses are likely in the tens of millions of dollars, if not more.

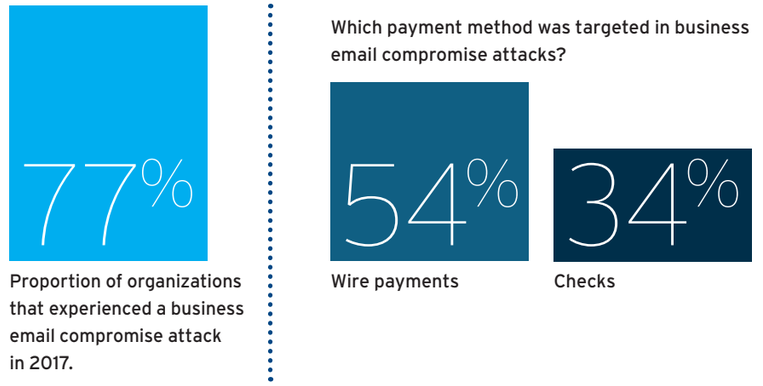
"The potential losses are huge," a 2017 report produced by the Economist Intelligence Unit (EIU) states. "Hackers infiltrating individual companies have stolen tens of millions of dollars in a single attack. The stock price of breached companies falls, and CEOs are sacked. Data losses create reputational damage and lawsuits from inside and outside the company. Even mergers and acquisitions can be derailed or altered in value to the tune of hundreds of millions of dollars."

Today's cyberattackers differ from previous generations in their meticulous planning. Criminals undertake copious research and trial-and-error experimentation in plotting the crimes before they execute. "Sophisticated cybercriminals use social engineering and inside information gleaned from lengthy reconnaissance within a given company's systems to execute high-value thefts," the EIU report states.

Nevertheless, many treasurers believe their companies are well-protected. To a certain extent they are—most organizations have undertaken basic security procedures like installing software system updates, limiting network and data access, and incorporating penetration testing to spot vulnerabilities. The Achilles heel in many cases is people. Even after small doses of cybersecurity training, treasury, finance, and accounts payable staff may fail to recognize (or respond effectively to) scams that use social engineering to target the right people with the right message for a successful attack. Thus, business email compromise remains the primary attack vector used to gain unauthorized access to treasury systems.

"The biggest threat to corporate treasury cybersecurity is often staff complacency," according to a report on treasury payment fraud by research firm IDC. "Cybersecurity within the treasury department is as much, or perhaps even more, about the people."

Business Email Compromise Scams



Source: AFP Payments Fraud and Control Survey Report 2018

A common example of a business email compromise attack that utilizes social engineering is the so-called "CEO fraud," in which a hacker, impersonating the company's CEO or other senior executives, emails a specific employee asking him or her to make an urgent, confidential payment on the executive's behalf. In some cases, the hacker follows up with a phone call to the person, who has been carefully selected as having personality traits that suggest he or she is unlikely to question authority.

Before an employee receives such an email, the scammer does a lot of research. Typically, these scams are perpetrated by someone with inside knowledge of the company, its business procedures, and key people, which enables the scammer to augment the appearance of legitimacy. These requests also emphasize the time-sensitive nature of the payment, which pressures the employee to act immediately and discourages him or her from seeking to substantiate the request with another senior executive before initiating payment.

If there is a silver lining here, it is that the relatively small number of treasury employees limits the available pool of people for scammers to target. "In an organization of 25,000 people you might have 10 or 15 people within treasury, narrowing a hacker's ability to perpetrate a phishing attack," says Stark. "At the same time, though this makes it easier to seek out the most vulnerable target."

How to Mount a Defense

Treasury organizations are extremely concerned about the risk of payments fraud. "This is not a question of 'Will this happen?'—it's a question of when," says Shenoy. "The majority of treasury professionals have seen payments fraud and other types of cyberattacks. Such attacks are increasing in number and sophistication. Regrettably, there is no silver bullet to stop all attacks at once."

Studies back him up. An overwhelming 84 percent of corporate treasury groups believe the threat of cyber fraud has increased over the past year, accord-

(continued on page 10)

Treasury Fights Back: Latest Trends in Combating Cybersecurity Threats

Cybersecurity threats have become so commonplace these days, that many of us barely raise an eyebrow when hearing about the latest attack. However, treasury professionals are the stewards of company finances and understand the potential high cost of such attacks better than most. They are rightfully concerned about the vulnerabilities of their organizations.

As the world increasingly embraces digital technologies, this ongoing evolution has coincided with an escalation in cyber threats. A recent report estimates that monetary losses globally from cybercrime are expected to reach a staggering $6 trillion annually by 2021. This is up from $3 trillion in 2015. This potential unprecedented monetary loss could very well negate the productivity and efficiency gains achieved through innovation and investments in next generation technologies.

These threats are pervasive, impacting corporations, financial institutions and public sector agencies everywhere in the world. Their impact comes in three broad categories. The most evident is the illicit theft of funds taken from accounts. Another form of cybercrime is the theft of data, such as trade secrets or increasingly valuable demographic information, which is the backbone of the burgeoning "big data" revolution.

The third form is disruptive attacks, such as ransomware that take businesses offline and prevent them from operating until a ransom is paid. Forbes estimates that a business falls prey to a ransomware attack every 40 seconds and such attacks are growing at a rate of 350 percent annually.

A smarter approach to cybersecurity

Effectively mitigating cyber threats presents complex treasury challenges. Simply erecting elaborate barriers to prevent intrusions could have the unintended consequence of reducing the accessibility and convenience of digital channels that organizations use to interact with banks and manage their finances and accounts. In other words, putting more locks on the door is not necessarily the best approach for preventing threats.

Citi is taking a comprehensive approach to cybersecurity, leveraging information gathered from the interactions between clients and the bank to develop tailored risk analysis in real time. Data, such as the date and time when clients normally log into the bank's platform are used in an effort to help detect unusual behavior. A login at midnight might indicate an unauthorized transaction, which triggers an additional security question to help confirm the identity and authority of the user.

Similarly, when a new device (such as a smart phone) that the bank doesn't recognize is used to access an account, extra controls should kick in to help verify the user has permission. Notification is also sent to the authorized user to ensure they know this new device is attempting to access the account.

Another piece of data that is analyzed is the geographic location of the person conducting the transaction. When IP address data is combined with date and time information, it becomes possible to flag any unusual changes such as a transaction happening in two widely dispersed geographic locations in a very short period of time.

Harnessing machine learning capabilities

Citi is taking things a step further by harnessing machine learning. Currently Citi is piloting a tool that applies machine learning algorithms to analyze client payments and help identify unusual activity. This is done by using advanced algorithms to compare new payments against an existing history of payments. Clients are alerted to any non-conformity with past trends on a real-time basis, so they can make more informed decisions on authorizing payments.

Machine learning can be an effective tool for speeding up the analysis process, while reducing the need for manual intervention. Also, as treasury organizations increase the automation of processes that rely on system-to-system connections with banks, solutions like these are helpful in terms of identifying unusual activity and allowing further scrutiny by clients.

One of the beauties of machine learning is that over time it can improve its own ability to correctly identify unusual activity by constantly refining the personal profile of each user. In this way, users aren't repeatedly inconvenienced for activity that is completely normal for them, whether it be traveling or working late at night.

Active and passive biometrics: The client becomes the key

The next wave of cybersecurity is leveraging both passive and active biometric information, in an effort to promote a stronger, more secure access and authentication process, while at the same time making it more convenient for clients.

Passive or behavioral biometrics is an extension of the previously mentioned data analysis strategy. Citi is using technology to understand the user interaction with the bank's systems in order to help identify atypical activity. For example, analysis can be conducted around behavioral patterns such as typing cadence or site navigation trends. Subtle, but distinct idiosyncrasies around how we work on our computers or mobile devices can be attributed to each user, thereby creating a profile. Conversely, when the user suddenly deviates from the profile, the system can understand that further attention is required to help ensure potentially unauthorized activity is not occurring.

All of this would take place in the background and would be completely unobtrusive to the user. It's important to note that Citi would only use this data for limited purposes as described above, and would never resell or externally share such behavioral data.

In addition to exploring potential use of passive biometric measures, Citi is looking to introduce active biometrics whereby, for example, when a client logs onto a desktop web portal, such as Citi Direct BE, they automatically receive a notification on their smartphone requiring them to verify their identity using the finger print or facial scan technology that is native to the phone. Once verified, the desktop app would then be activated.

The never-ending cybersecurity battle

Completely eradicating cyber threats is essentially impossible. Staying ahead of them is the more realistic goal. Citi is fully committed to employing the latest technology advances to help protect client and bank assets. Examples of this commitment include Citi's Cyber Security Fusion Centers in the U.S., Europe and Asia, which work day and night to help improve security functions and become smarter at anticipating future threats, so the bank can be more effective, and faster in responding to them.

For treasury professionals, the goal is not necessarily to become a cybersecurity expert, but rather to develop a strong working knowledge of the potential threats, as well as the tools and techniques available to help combat them. Being able to set the right controls and mitigate risks wherever possible is absolutely vital. Citi is here to help.

ing to a 2018 survey of more than 300 treasury professionals by consultancy Strategic Treasurer. "Fraud continues to be at the forefront of practitioners' minds, and security remains a top priority for treasury in 2018," the report states. "Fraudulent techniques such as business email compromise and ransomware have become the norm."

Whereas only 8 percent of respondents had experienced a ransomware attack in 2017, 25 percent had experienced at least one such event in 2018, a more than 300 percent year-over-year increase. Additionally, one-third of the respondents said they were not sure of the source of the attack—whether, for example, it originated internally or externally, and whether it involved a criminal working solo or a group.

Despite the extraordinary increase in cyber fraud threats, only one-quarter of corporate treasuries in the survey indicated that they have increased their spending on payments fraud security and controls in the past three years. Those that have primarily targeted treasury payment controls, reconciliation features, account-level controls, and fraud monitoring. The report concluded that many practitioners had inadequate security controls, unassigned fraud management responsibilities, a piecemeal approach to security, and poor visibility into transactions.

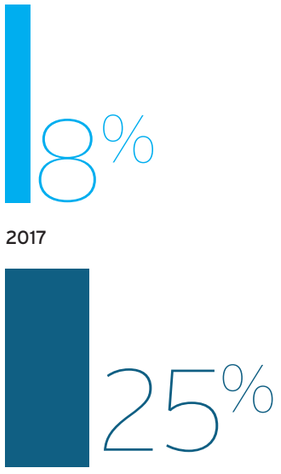
The latter finding resonates loudly with Stark. "Organizations continue to rely on human eyes to enforce payment policies," he says. "People can make mistakes, especially as they take on more responsibilities and have to review more data, or match payments against more fraud scenarios."

Building Resilience

In many corporate treasuries, the level of preparedness to identify and respond to future payments fraud schemes is unsettling. Fortunately, several well-known best practices can help treasury teams mount a stronger defense against cyberattacks.

Ransomware Reports Grow 300%

Proportion of treasury professionals whose company has experienced a ransomware attack in the past year.



*Source: Strategic Treasurer 2018 Treasury Fraud & Controls Global Survey *YTD*

The first step is to identify major vulnerabilities in the corporate network and treasury-related systems. Through in-depth risk assessments, the company's information security team and/or an external cyber-risk consultant can ferret out weaknesses in the treasury organization's critical business processes, data assets, and systems, as well as the integration points between systems.

Citi's Treasury and Trade Solutions team utilizes regular cybersecurity reviews. "It is critical to have the right subject matter expertise to pinpoint vulnerabilities and know how to effectively respond," Shenoy says. "We work hand-in-hand with teams across the organization to safeguard our most important data on a day-to-day basis. Our information security team also analyzes recent cyber events as well as real-time threat intelligence to assess potential impact to the treasury system and our processes."

Based in part on these analyses, Citi recently strengthened the security of its client-facing online platform. Customers using its banking services app can utilize a software token that generates a one-time password on their mobile device for authentication purposes. "We've also put in place invisible controls that the bad guys are unaware of, using advanced analytics and machine learning technology to help identify a customer's normal patterns against what appear to be anomalies," Shenoy says.

When unusual activity occurs, such as a customer logging onto the platform at an unusual hour or from an odd location, the system sends up a red flag. "We're not expecting to catch 100 percent of fraudulent activities, but we'll expect to catch more of them," Shenoy says.

Stark agrees. "AI-based payment fraud detection is increasing in sophistication, with complex algorithms now able to detect custom fraud scenarios in real-time," he says. "In some cases, these tools are built into payment workflows, building a better line of defense."

Another best practice is to conduct routine penetration tests to uncover weaknesses in the cyber-defense methods of the treasury organization, suppliers, and partnering organizations. The EIU report indicates that 92 percent of respondents to that survey conduct internal penetration testing, but only 33 percent apply the same testing to their suppliers.

Moreover, 19 percent of treasury departments fail to check their suppliers' identity authentication processes or evaluate whether suppliers have secure email systems for protecting confidential information. "Our research found serious gaps in corporate defense, including vulnerabilities hidden within third parties and their subcontractors," the EIU report states.

Stark affirms that third parties are a chink in the armor. "We find it highly advisable for the CISO or someone in information security to require suppliers to fill out a lengthy questionnaire asking them about their IT security processes," he says. "This way, you're able to compare each supplier against other suppliers in terms of their cyber-risk defenses and response procedures. The more vulnerable suppliers become that much clearer."

Workflows and Controls

Another smart tactic is to standardize and document payment approval workflows and other treasury processes, and to appraise the effectiveness of these controls on a regular basis. "There are information security standards like ISO 27001 and third-party audits like SOC 1, 2, and 3 reports that treasury technology vendors should adhere to," Stark explains.

Two other defensive processes are to encrypt all treasury data in transit and at rest, and to segregate duties within the treasury organization to reduce the possibility of internal fraud. With regard to the latter tactic, only certain people should have access to specific types of payment data.

"You want to separate the duties between the payment initiator, the payment approver, and the reviewer of a detected payment," says Stark. "It's best to designate these reviewers by payment rule and specific payment scenarios. For example, a decision might be made for payments under $1 million to be reviewed by the treasury manager, whereas payments over this amount would be sent to the treasurer for review."

Yet another best practice is to use a security incident and event management (SIEM) system. The InfoSec Institute describes SIEM systems as offering a "real-time analysis of a security alert generated by operational systems, applications, network hardware, and databases."

"If you don't have a SIEM system and you're hacked, you're likely to be stuck wondering too long about what you need to do next," says Stark. "The longer you wait, the worse the situation can become. And if the attempt is successful, it is typically followed by additional attacks." He pointed out that Kyriba's cloud-based treasury solution comes equipped with a SIEM system.

Help Is Here

Many companies that provide products or services to corporate treasury functions are offering online resources that help customers with cyberattack planning, management, mitigation, and response. For instance, both Kyriba and the Treasury and Trade Solutions group at Citi have created guides to help detect various scams.

Corporate treasury teams will become increasingly effective at discerning and defending against cyberattacks as cutting-edge technologies become more widely available. "Later this year, we plan to roll out tools that have the potential to detect anomalies in how users navigate applications using their computer mouse, arrow keys, and the scroll bar," says Shenoy. "Such behind-the-scenes tools can tell us things we couldn't guess at before."

Just in time, too. "Cyberattacks are becoming more sophisticated, but we're becoming more sophisticated, too," says Stark. "Our capabilities are constantly improving." T&R

Russ Banham is a Los Angeles-based freelance business writer and author specializing in the intersection between finance and technology.

TREASURY&RISK

THE FUTURE OF FINANCE TODAY

PROVIDING CRUCIAL INFORMATION FOR MANAGING A CORPORATE TREASURY FUNCTION ON A DAILY BASIS.

Check out these recent articles from *Treasury & Risk* written for Corporate Treasury and Finance Managers like you:

- **How BEPS Will Affect Treasury.** The BEPS Project from the OECD and the G-20 requires multinational companies to review, and perhaps reconsider, some of their core treasury structures.
- **5 Points About Same-Day ACH.** Using the speedier payment method will be optional, but treasurers must be ready to accept such payments.
- **Managing Treasury Across the U.S.-Canada Border.** Here's how to navigate the two nations' differences in treasury practices and banking processes.
- **The Controls Sanity Check.** Why you need to rethink your financial controls—and how to go about doing so.
- **Connecting to SWIFT via a Service Bureau.** Why international development agency OFID chose the service bureau route, and how the decision has transformed its treasury.
- **How to Win Board Approval for a Hedge Program.** Six ways to improve the odds that your presentation to the board of directors will result in a green light for your FX hedging plan.
- **Switch to "True" Working Capital Metrics.** Technology today enables companies to get a more realistic understanding of their performance in working capital management.

Receive top stories like these from *Treasury & Risk* straight to your inbox, free of charge, via our weekly eNewsletter, *T&R Express*, and our bimonthly special reports.

Go to treasuryandrisk.com/enewsletters to subscribe today!

ALM