SPECIAL REPORT: CYBERSECURITY

TREASURY&RISK

THE FUTURE OF FINANCE TODAY

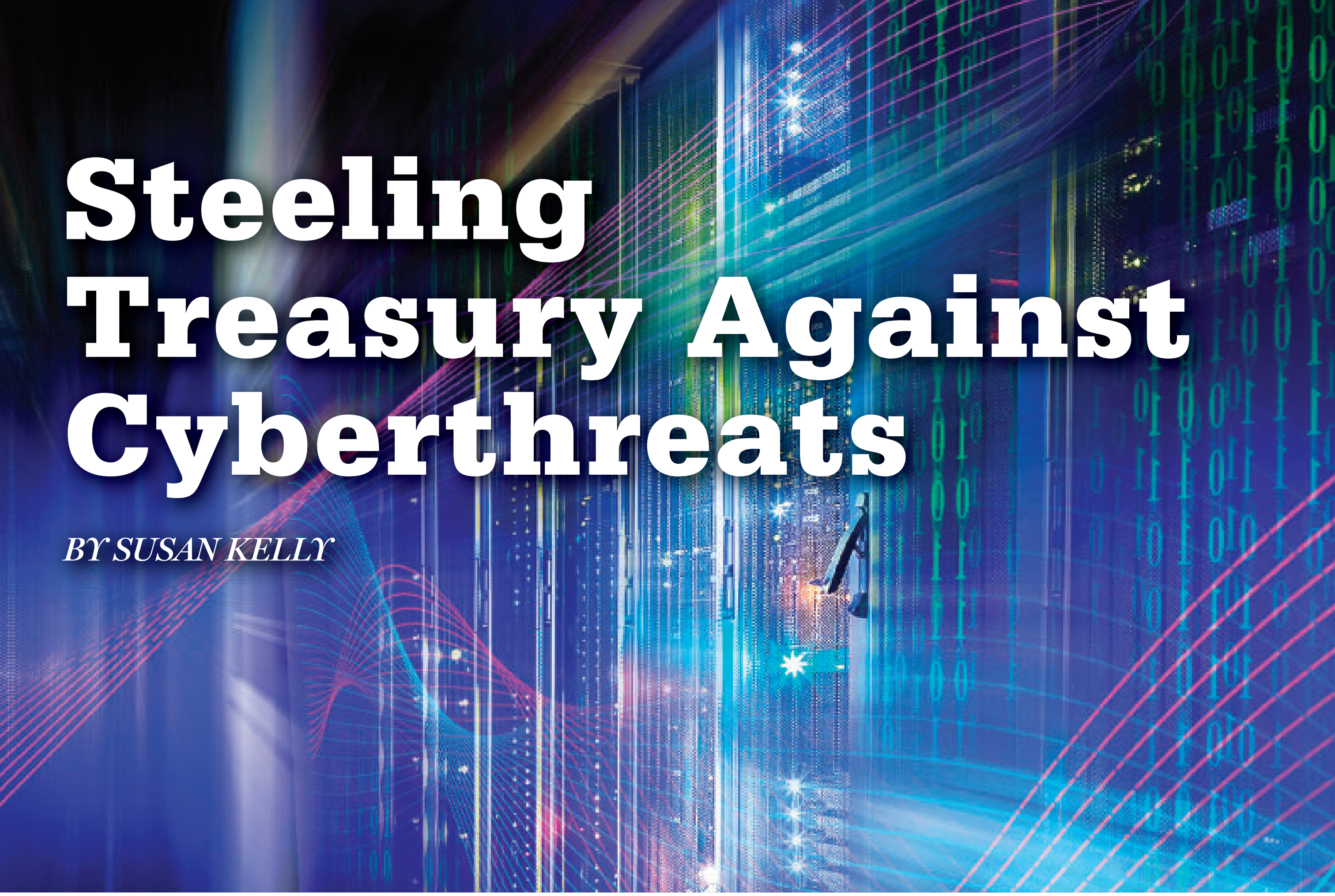
Steeling Treasury Against Cyberthreats

PAGE 2

Sponsored by Openlink and Strategic Treasurer

NOVEMBER 2017 SPECIAL REPORT • treasuryandrisk.com

An ALM Publication



Steeling Treasury Against Cyberthreats

BY SUSAN KELLY

Cyber risks are escalating as the price tag attached to cybercrime explodes. While many of the incidents recently in the headlines involved data breaches and ransomware, the risks that face corporate treasuries in particular have been brought home by the mounting costs of business email compromise scams and cyberthefts that involve the SWIFT financial messaging system.

Most notably, hackers stole $81 million from Bangladesh's central bank last year by penetrating the system the bank used to access SWIFT and sending fraudulent payment instructions.

In May, the FBI estimated that business email compromises—scams in which cybercriminals trigger unauthorized payments, often wire transfers, by sending emails that appear to come from a company executive—caused $5.3 billion of losses globally from 2013 to 2016, and U.S. losses of $1.6 billion over that same time frame.

"There's definitely a raised awareness and concern," said Craig Jeffery, managing director at Atlanta-based consultancy Strategic Treasurer.

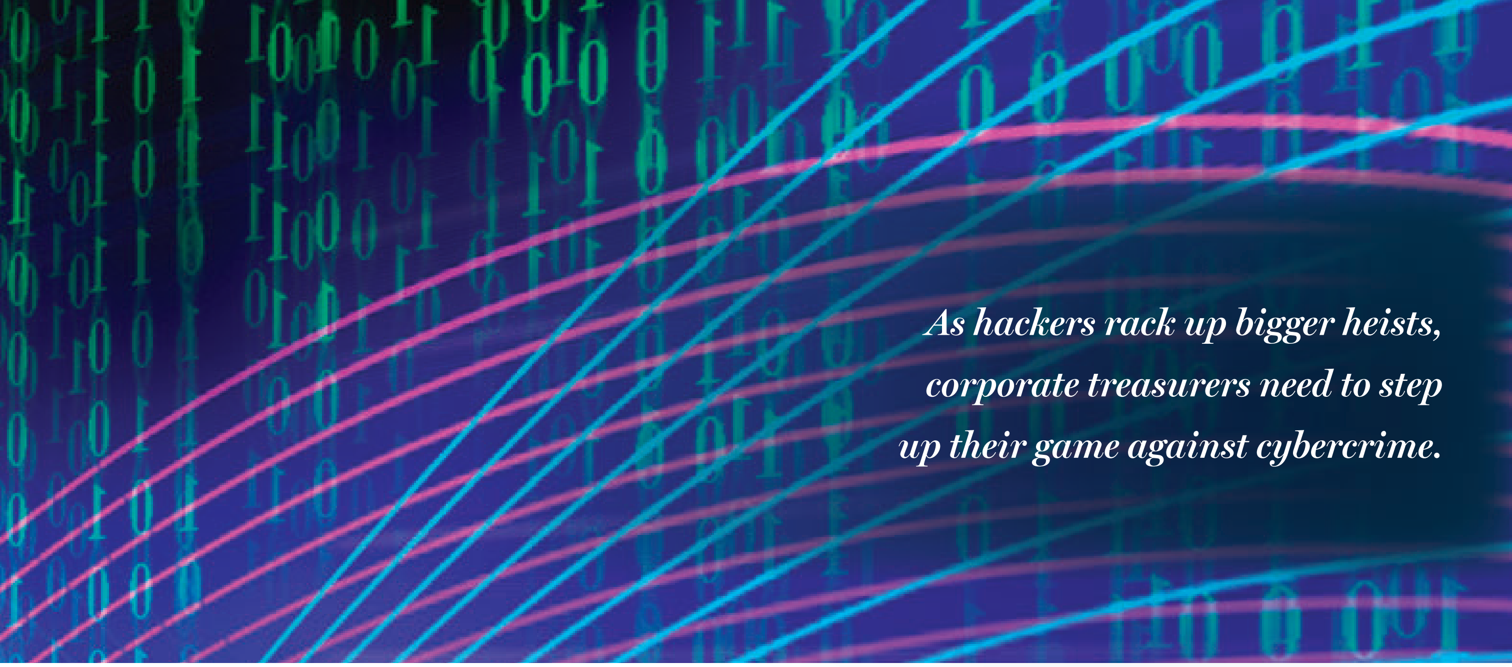
The hit that a single company potentially could suffer is no longer the $1,500 average for check frauds or even the $130,000 average for a business email compromise, Jeffery said. Losses "are getting larger; they're getting significantly larger.

"People need to understand the scope of the losses that everyone's experiencing," he added. "This absolutely requires a much more aggressive posture, a stronger, more muscular approach to defeating that. The calculus changes. It becomes too expensive."

Business email compromise (BEC) scams are also notable for their prevalence. Seventy-nine percent of companies said they had experienced business email compromise attempts over the past two years, according to a survey conducted earlier this year by Strategic Treasurer, Bank of America Merrill Lynch, and Bottomline Technologies. Twelve percent of overall respondents, and 15% of those who had experienced a BEC attempt, had suffered a loss.

"These are organizations that are patient," Jeffery said of the hackers. "They'll surveil organizations through social media, they'll compromise credentials, they'll sit and monitor how things are done over time, and they'll use that knowledge to violate whatever the policy is."

While treasurers are concerned about


As hackers rack up bigger heists, corporate treasurers need to step up their game against cybercrime.

cyberthreats, Jeffery said they may not be concerned enough.

"There's always a bit of a lag when something happens," he said, and cited the example of the SWIFT Customer Security Program, under which users of the messaging network now have to attest each year to their compliance with a set of security standards, with the first deadline Dec. 31. "Too often, we've heard companies saying, 'What if I don't attest? Is that a problem? I have a lot of other things to do,'" Jeffery said.

Jeffery noted that corporate treasuries are planning to spend significantly more on technology in response to the risk. Strategic Treasurer's 2017 survey showed 61% of companies said security concerns had a strong or very strong influence on their plans for technology spending.

Payments

Jerald Seti, vice president of product management at Openlink, a trading, treasury, and risk management solution provider, said he was seeing particular concern around payments given the thefts involving SWIFT.

"That's definitely raised the attention of treasury in terms of locking down their payments mechanisms," Seti said, and added that a fraudulent payment can have an immediate impact on a company's finances. "One payment can go out, add a couple of extra zeros, and a firm can be bankrupt overnight," he said.

The Strategic Treasurer survey showed 46% of companies surveyed had higher or significantly higher payment security concerns in 2017 compared with 2016, while just 2% had lower concerns.

Seti said cybercrimes involving corporate payments have increased corporates' interest in encrypting payment files. "Treasurers that are looking at new systems are definitely requiring encryption as a way to handle that risk," he said.

If hackers can get into the message files that contain payment instructions, they have access to bank account numbers and amounts of payments. The SWIFT network is fortified, Seti said, so "it's when a file is dropped, produced by a system and waiting to be picked up by a delivery mechanism, that it should be encrypted. Or if you're sending the file to a service bureau, you probably want to encrypt it as well.

"By encrypting it, either by totally obfuscating the data inside that file or adding a key that would validate that no single byte in that file has changed, you can mitigate the risk that someone has actually touched that file," he said.

Sayantan Chakraborty, head of product management for Global Treasury Management at U.S. Bank, also noted corporate treasuries' use of encryption, both to secure connections and encrypt the data being transmitted.

Treasuries also want to be notified if anything odd happens in a bank account, Chakraborty said, and want to know whether bank platforms have that capability, including a workflow that sends information to the correct person, who can then take action. "They're trying to get information in a faster and proactive fashion, so if something appears out of the ordinary, they can take action around it," he said.

> "People need to understand the scope of the losses that everyone's experiencing. This absolutely requires a much more aggressive posture, a stronger, more muscular approach."
>
> —CRAIG JEFFERY, STRATEGIC TREASURER

The U.S. is moving toward faster payments, he noted. "As the velocity of payments increases, it becomes even more important to ensure [users] are monitoring them in near real-time."

SWIFT's Customer Security Program, or CSP, sets out 27 security controls, 16 of which are mandatory, and requires customers to comply with all of the mandatory controls and attest to their compliance each year.

Strategic Treasurer's Jeffery predicted other payments networks will roll out security

(continued on page 6)

SPONSORED STATEMENT

Six Steps to Secure Your Treasury & Risk Operations

By Jerald Seti, VP Product Management, Openlink

Batten down the hatches. Fill the moat. Close the drawbridge. These are old concepts but relevant just the same in the digital age. With cybersecurity moving to the forefront of corporate concerns, there's a lot that end-users can do to help prevent a debacle from occurring within their organization. At times, it seems like this is an IT problem to solve, however, there are a multitude of steps that can be taken by end-users.

First, look within your mission critical applications and take advantage of all the security capabilities inherent in the product. Do your systems provide permissions and settings for individual users at a very granular level? Good systems have separate write, update, delete and view database permissions. Don't be lazy. It's essential to set up a tight security profile that gives users just enough latitude to get their jobs done AND keep them and your business out of trouble. Secure user controls by saving role profiles as master settings that new users with the same functional responsibilities can inherit in the future.

Second, lock down your business processes. Apply "4-eyes" approval workflows to virtually everything. Hopefully your system is flexible enough to set up flexible authorizations based on thresholds and filters. For example, payment outliers above a certain amount or in "unusual" currencies should be automatically flagged and subject to additional approvals.

Third, reexamine all of the spreadsheets you use and try to integrate their functionality into your enterprise system. Do you still use spreadsheets to manage collateral and margin? Are you running macros to perform complex performance measurement benchmarks? Spreadsheets provide tremendous opportunities for bad outcomes. They're not secure, tend to be shared and replicated, contain confidential information and complex formulas with potential errors that are not vetted in the same manner as enterprise applications, and they tend to lack documentation.

Fourth, take a critical look at your entire operation. Vulnerabilities abound that you may not have considered. What artifacts (log files, back up files, payments messages, reports) are left behind which contain critical information? Are they encrypted? Can they be eliminated? Can they be stored in a more secure location? Is access permissioned?

Fifth, how secure is your payments ecosystem? A rogue or missed payment can have a huge impact on reputational risk. SWIFT has issued a protocol that its members will need to subscribe to starting in 2018. Has your organization reviewed the changes and started addressing their implementation? If you use a bank portal or TMS, take advantage of every security protocol they offer ("4-eye" approvals, repetitive and semi-repetitive templates, encryption, etc.).

Sixth, do you have the system capabilities in place to create centers of excellence for your key business processes? Can you mitigate the risks of dispersed, non-centralized responsibilities? For example, do you have a handle on global bank statements? Can you detect a rogue payment in near-real time and prevent additional damage? Is there a secure golden copy of your reference data, parties, and bank account information locked down in a tightly permissioned central repository?

As you can see, cybersecurity goes beyond just firewalls and encryption devices. It's up to all of us to help protect ourselves and our companies from nefarious actors as well as manual operational errors. So batten down the hatches, fill the moat and close the drawbridge on these security issues by examining all your vulnerabilities, from simple spreadsheets to complex business processes. Email us at info@openlink.com if you'd like some help.

6 Steps to Secure Treasury & Risk

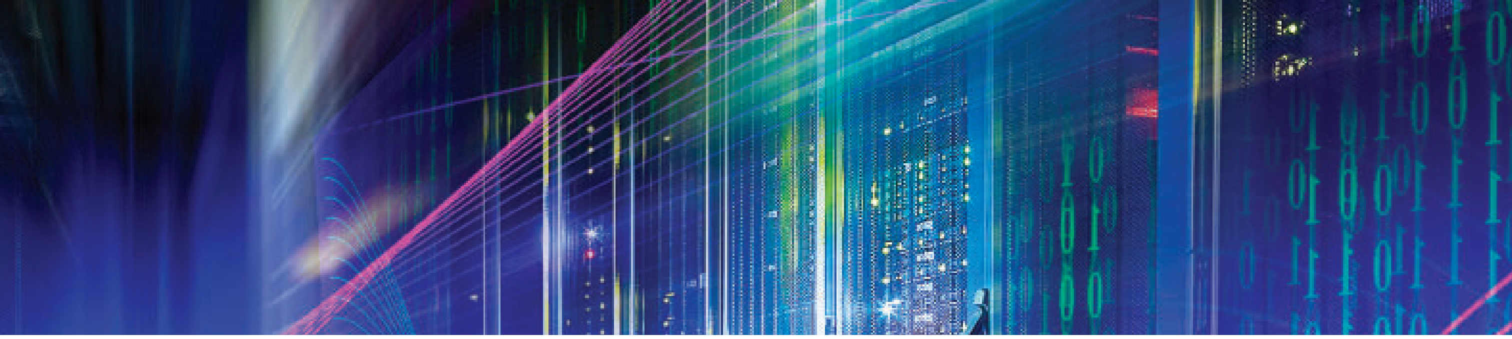
1. **EXAMINE** security features in your systems
2. **ADD** controls such as 4-eye approvals
3. **MOVE** spreadsheet functionality into your system
4. **AUTOMATE** operations to reduce vulnerability
5. **SECURE** your payments process
6. **Create** centers of excellence for key processes

Is your organization a technically secure fortress capable of fending off enemies in the 21st century?

At Openlink, we take security very seriously by providing permissions, encryption, authorization workflows and cloud hosted solutions that are part of a complete arsenal needed to mitigate operational risks and protect cybersecurity.

Six steps to secure treasury and risk

1. Examine security features in your systems
2. Add controls such as 4-eye approvals
3. Move spreadsheet functionality into your system
4. Automate operations to reduce vulnerability
5. Secure your payments process
6. Create centers of excellence for key processes



CYBERSECURITY (cont'd from page 3)

standards for companies that use their solution to make payments. “We think that's going to become the norm,” he said.

Industry Standards

Chakraborty argued that adopting industry-standard protocols, such as encryption standards, file formats, and transmission standards, is a step in the right direction when it comes to treasury cybersecurity.

Such standard applications make change management easy. “When you have an update to a standard, it's much easier to deploy it across the board,” he said, and since standard applications are usually backed by consortiums or large institutions, “there's a shared interest in keeping them updated.”

He cited the ISO XML standard for financial messages as a good example. While corporate customers traditionally communicated with their banks using proprietary file formats, “there's a concerted move we see toward ISO XML formats,” Chakraborty said. Other examples include secure FTP for file transfers and application programming interfaces, or APIs, to connect with service providers, he said.

Spreadsheets a Weakness

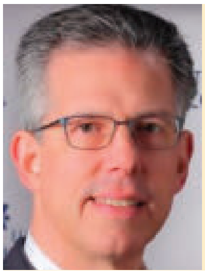
Seti argued that treasury departments' “most glaring” weakness when it comes to cybersecurity is their continued reliance on an older form of technology: spreadsheets.

The use of spreadsheets “just creates a whole bunch of vulnerabilities on many different levels,” he said.

For starters, employees usually send spreadsheets back and forth in emails, and emails can contain viruses, he noted. And the fact that spreadsheets can be emailed means a loss of control from a security perspective.

“If you're a security officer and you're trying to impose compliance rules, you can permission certain screens,” Seti said. “Spreadsheets are the Wild West—you have no control over who's viewing the data, or who sent the data to whom.”

He pointed to the macros inside spreadsheets, which can be infiltrated by a virus or contain typos, whether intentional or unintentional, as another source of risk. There's also the danger of having a laptop stolen that contains spreadsheets with confidential information, such as Social Security numbers.



> “Spreadsheets are the Wild West—you have no control over who's viewing the data, or who sent the data to whom.”
>
> —JERALD SETI, OPENLINK

Spreadsheets are “still pervasive; they probably won't go away—but it's wrong,” Seti summed up.

Cloud or Not

More and more corporate treasury teams are shifting to technology that's hosted in the cloud, which allows for quicker and easier implementations and updates, and may lower costs. Some argue that cloud solutions are also a plus when it comes to guarding against cyberthreats because cloud providers are likely to employ better cybersecurity measures than an individual corporate would use for its on-premises software.

“Those environments are fortified as a common way of business,” Seti said. “That's the point of them: to have every security precaution taken care of.”

Cloud vendors enjoy economies of scale that benefit their security measures, said Thomas Hunt, director of treasury services at the Association for Financial Professionals. “They've probably got a higher echelon of security than a corporate on its own could adopt,” he said. “It wouldn't be cost-effective.”

But Drew Del Matto, CFO of Fortinet, which provides cybersecurity software and services, said cloud solutions can still entail challenges when it comes to cybersecurity, although their challenges are different than those related to installed software.

“Many organizations have multiple security-vendor products in their infrastructure, with different operating systems and solutions for the cloud,” Del Matto wrote in an email. “This can create a visibility, control, and management challenge for cloud-based applications and workloads.”

Del Matto said that “if the right type of security architecture is in place, cloud-based solutions can actually provide the same level, if not better, security.”

With software-as-a-service offerings, “it can actually be easier to apply controls such as data loss prevention, two-factor authentication, etc.,” he said. “Also, cloud-based applications can deliver great auditing, reporting, monitoring, and email security solutions for treasury departments looking to offload some enterprise workloads to the cloud.”

David Watson, global head of digital cash products for Deutsche Bank, noted that not all cloud solutions are the same. “Cloud A does not necessarily have the same level of security as Cloud B,” he said, so companies still need to assess how secure the environment is when they're selecting a vendor.

Jenny P. Menna, a senior vice president and cybersecurity partnership executive at U.S. Bank, said the cloud “can be extremely secure.” But she cited a list of factors that treasuries should

be sure to consider when shopping for a cloud solution, including how the cloud provider handles incident response, what the contract says about who has access to the company's data, and, if the cloud is shared, what barriers exist between the company's data and that of other tenants.

Another issue to consider is where the data will be housed. "Depending on which legal jurisdiction data is housed in, that may create some unique situations for the company if something goes wrong," said U.S. Bank's Chakraborty. Treasury should be sure the company's lawyers look at where the data to be stored in the cloud will be located and what issues might arise in that jurisdiction.

Centralization

Centralization, or the lack thereof, is another element that can affect a treasury's cybersecurity.

In larger organizations that have many affiliates spread out around the world, a single type of treasury work may be performed by many different parts of the organization. Openlink's Seti cited the example of a company with 10 different groups that make their own payments. In that situation, "I kind of lose control over the whole process if I'm the global treasurer, " he said. "I don't know what they're doing; I don't know how well they're protecting the data.

"The name of the game here is to centralize all these processes," he argued.

"We took an insurer with 1,500 bank accounts around the globe, making thousands and thousands of payments on a daily basis from six or seven payment centers, and moved them all into one payment center," Seti said. "That gives you much better control, not only of the operational aspect but the forecasting aspect, and enables you to see anomalies that might be happening."

Strategic Treasurer's Jeffery said cloud services can serve as the path to such centralization.

"Let's say you have a payments hub, and now you're routing everything from multiple payment areas through the hub," he said. That move not only increases efficiency and improves forecasting, "you can be sure you're looking in one key location where all the money is moving through."

Centralizing the payments also decreases risk, he said, since "you're moving information from 50 locations, each of which can be penetrated, to a single location."

"Education is a key first step. Phishing attacks, triggered by employees clicking on malicious links, are still one of the greatest cyberthreats."
—DREW DEL MATTO, FORTINET

Similarly, centralizing certain activities in a shared service center "means there should be more expertise," Jeffery said. "Someone who's handling these types of payments all the time, they're not going to be as readily fooled" as a staffer who's doing 20 different tasks in the course of the day.

He noted that while approaches like shared service centers or centers of excellence should provide more security, they have to be properly implemented.

Treasury's Role

Treasurers should use a framework that looks at the four elements of IT security: the company's IT perimeter, its interior security, the transport function, and its third-party providers, Jeffery said.

"Even though the perimeter might be largely IT's domain, treasury needs to know about that," he said. Treasury should regularly review what they're doing and how each of those elements is being assessed, Jeffery said, and suggested that some of those reviews should be by an external party, rather than internal audit.

But to what extent does treasury have the authority to oversee IT security outside its domain, or the resources to do so? Few treasuries have dedicated IT resources; most have to request the help they need from the IT and information security departments, which report up to other parts of the organization.

Jeffery said treasury should be "the superintendent of security.

"That doesn't mean they're in charge of who locks the door or selects which antivirus software or what exact tools are used to protect the perimeter," he said. "But as superintendent, they are responsible for protecting the corporate assets.

"To me, they should be asking IT and the information security people: 'What are we doing to protect the perimeter, how is that changing, what are the attempts we're getting hit with?'" Jeffery said. "They should be getting that information, and they should be understanding it to a certain extent and taking the view that they are the superintendent of it."

Others see the process as a partnership. "It's critical that treasury be actively involved in thinking about the issues and partnering with the IT department, because they're the ones who have to make IT understand, 'This is what's important to us,'" said U.S. Bank's Chakraborty.

Treasury executives should be "proactive, rather than reactive," said Fortinet's Del Matto, and work with executives in IT and information security "to ensure that the company's security architecture can rapidly detect, isolate, and mitigate any breach."

Deutsche Bank's Watson said while corporate treasurers are highly aware of cyberthreats at this point, their views on what

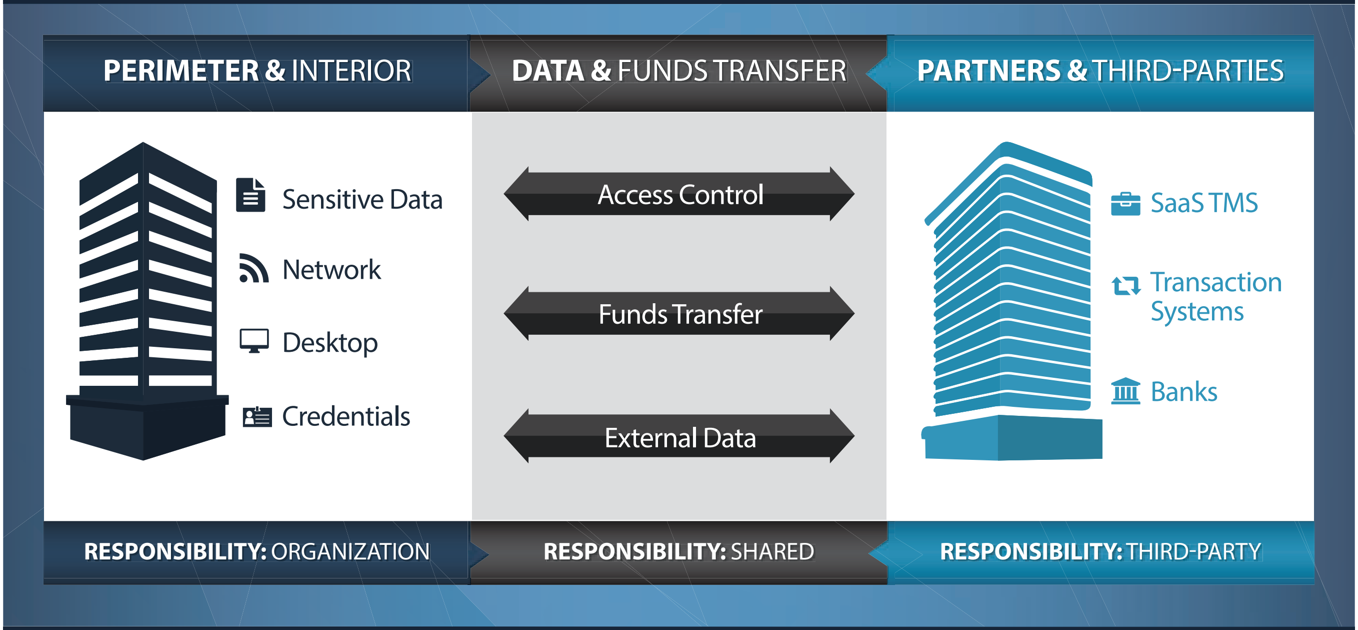
(continued on page 10)

STRATEGIC TREASURER
Consultants in Treasury

ADVISING CLIENTS,
INFORMING THE INDUSTRY

StrategicTreasurer.com

THE FRAUD LANDSCAPE: CORPORATE TREASURY EXPOSURES



PERIMETER & INTERIOR

Sensitive Data

Network

Desktop

Credentials

RESPONSIBILITY: ORGANIZATION

DATA & FUNDS TRANSFER

Access Control

Funds Transfer

External Data

RESPONSIBILITY: SHARED

PARTNERS & THIRD-PARTIES

SaaS TMS

Transaction Systems

Banks

RESPONSIBILITY: THIRD-PARTY

CYBERCRIME: TREASURY IN THE CROSSHAIRS

1 Fraud is an Industry Pandemic

In a recent Strategic Treasurer survey, 86% of organizations indicated that they had been targeted by fraud within the past two years, either through payment fraud, cyberfraud, ransomware, or BEC attacks. For successful attempts, the payouts for criminals ranged from hundreds to millions of dollars.

2 The Criminal's Playbook is Sophisticated

Rather than rely a single tactic, criminals were found to utilize a vast number of fraud techniques that targeted multiple exposure points through automated software. These techniques often extended beyond the boundaries of an organization to include their business partners and third-party vendors.

3 The Age of Tech-Savvy Criminals

While physical fraud continues to be an issue, a growing concern amongst organizations is the rising technological expertise of criminals. Within the past two years, 79% of firms experienced at least one Business Email Compromoise (BEC) attack, with 15% of targeted firms suffering a loss. Additionally, 45% of organizations experienced cyberfraud attempts within the past year.

4 Employee Credentials are Vulnerable

As criminals continue to evolve, they are increasingly targeting the credentials of key personnel within organizations as a mechanism for perpetrating fraud. The scope of this activity commonly includes treasury staff, due to their position over funds transfer activity and bank account information.

5 Treasury Personnel are Key Targets

As fraudulent schemes continue to hit the landscape, treasurers and other financial personnel have become the preferred targets for criminals, who regularly use BEC schemes, phishing, malware, and other mechanisms to steal information, gain access to the organization's network, and ultimately, extract funds.

6 Fight Exploitation with Education

In order to protect their data, assets, and information, organizations must ensure that their employees are aware of the latest fraud schemes and techniques, and have received proper training on how to successfully identify, prevent, and respond to attacks. This training must be provided regularly, so as to keep pace with the constant evolution of the fraud landscape.

SecureTreasury™

IGNORING THE THREAT IS **NOT AN OPTION**

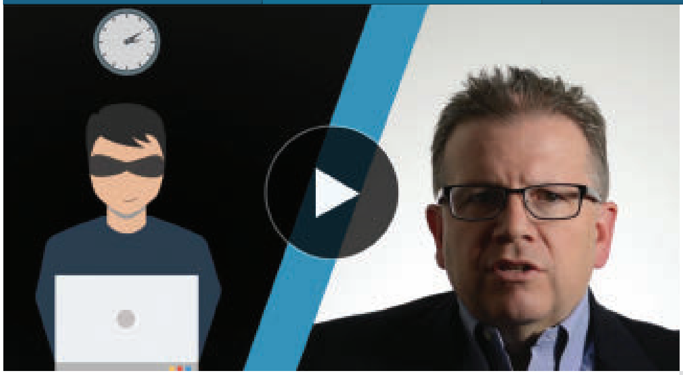
EMPLOYEE **TRAINING**

TREASURY SECURITY

ONLINE VIDEO **COURSE**

TRAINING · TESTING · DOCUMENTATION
Persistent · Updated · Subscription-Based

Increased **Awareness** | Greater **Knowledge** | Fraud **Prevention** | Risk **Mitigation** | SWIFT **CSP**



Treasury Security Course

A professional cloud-based training course designed to reduce the risk of corporate payment fraud by educating interdepartmental staff on common approaches to fraud, areas of organizational vulnerability, and leading practices for increased controls within a complete treasury security framework.

✓ Proactive

Be prepared for fraud attacks before they strike.

✓ Efficient

Train your team at a global scale for a local cost.

✓ Continuous

Keep all employees up-to-date on awareness.

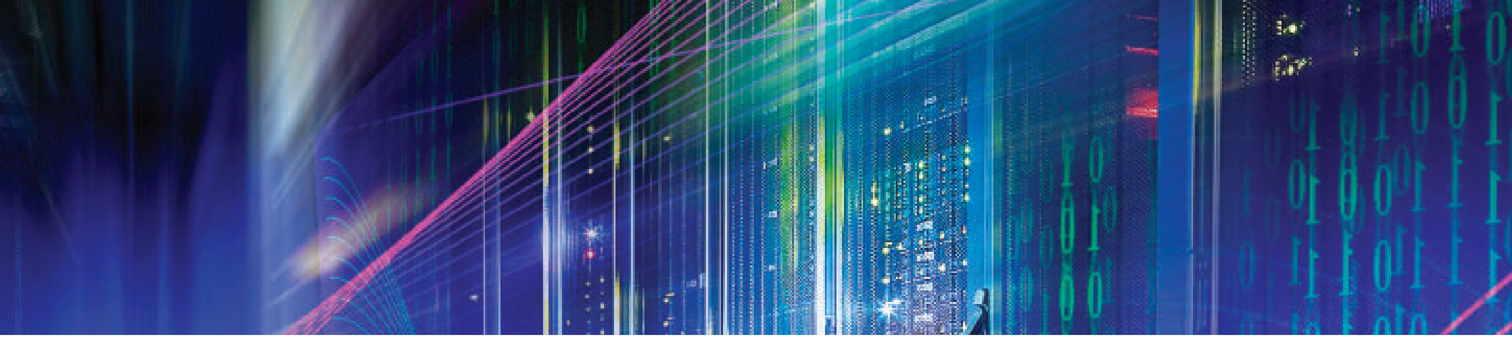
The Need for Training

1. Fraud is on the rise. It is growing in frequency and complexity. Criminal payouts are greater than ever.
2. All organizations are at risk. If you're not currently under attack, you're certainly under surveillance.
3. Awareness is a crucial line of defense against the risk of critical loss. Know how to spot fraud attacks.
4. **SWIFT CSP** requires annual staff training.

STRATEGIC TREASURER
Consultants in Treasury

ADVISING CLIENTS,
INFORMING THE INDUSTRY

CALL TODAY!
+1 678.466-2220
SecureTreasury.com



CYBERSECURITY (cont'd from page 7)

they can do about those threats vary.

Some understand that their role managing the company's funds means they should take the lead on "ensuring the right controls are in place on payments and money," Watson said. "At the other end, many treasurers see this as the role of IT or their corporate security office and haven't woken up to the fact that as the owners of the funds, they need to be in the driver's seat with their CISO [chief information security officer] and IT departments."

He rejected the notion that treasurers lack the power to influence the company's cybersecurity efforts.

"Is a corporate treasurer able to find out who their CISO is and go and challenge them on security tools?" Watson asked. "When the treasurer drives an RFP with banks, are they empowered to include the CISO in that process to define what questions to ask their banks, or include the CISO in their regular reviews regarding controls banks have in place?"

Treasurers "need to stand up and put themselves in the driving seat," he added. "They won't be asked to get into it."

He added that while having dedicated IT resources lets treasuries position themselves at the cutting edge of industry movements such as XML and state-of-the-art treasury management systems, developers who work on treasury issues aren't necessarily experts on cybersecurity.

Even a treasury with dedicated IT resources will "still need to work closely with a CISO team and understand what they should be doing when it comes to cybersecurity," Watson said.

The Human Touch

While improving security around treasury systems and processes is important, a large part of protecting treasury against cyberthreats has to do with ensuring that treasury employees are on guard against hackers.

Certainly in the case of business email compromise scams, it's employees who are clicking on links in emails or taking at face value a message purportedly from an executive such as the CFO.

"Education is a key first step," said Fortinet's Del Matto. "Phishing attacks, triggered by employees clicking on malicious links, are still one of the greatest cyberthreats.

Security Best Practices for Treasuries

From two-factor authentication and segregation of duties to automated reconciliations

There are many best cybersecurity practices that treasury executives can follow within treasury.

One easy step treasurers can take is to set up a dedicated computer on which treasury initiates all fund transfers, a computer that can't be used for email or surfing the Web, said Craig Jeffery, managing director at Atlanta-based consultancy Strategic Treasurer.

Treasury staffers should also practice "desktop hygiene," he said, which includes not keeping account information on employees' physical computers and making sure PCs and laptops have antivirus software and are regularly scanned and checked.

Laptops and other mobile devices should have encryption that would protect any corporate data in the event that the devices were stolen, Jeffery said. And users of laptops should protect against an unauthorized person using a flash drive to download data from the laptop.

Jeffery also cited the advantages of automated reconciliation. "If you have it automated, every day files are being compared," he said. If there's been some type of scam or cybertheft, "you will find the problem much more rapidly, and when you find it much more rapidly, you have the ability to contact the banks, and you may be able to get it frozen wherever it is and explain and get your money back."

Jerald Seti, vice president of product management at Openlink, pointed to several best practices corporate treasuries should follow, beginning with being aware of the security aspects of the software treasury uses.

Treasuries should be sure to use permissioning, rather than giving employees permission to do everything on a given software system. "They need to go through, role by role, and make sure permissions are granted or taken away at a very granular level," Seti said.

Treasuries should also use be sure to employ dual authorization. "They want to be sure they implement four eyes or more," Seti said. "Before a deal moves into the middle office or when a payment is keyed into the system, you probably want to have someone else just validate, review it, verify

“As the velocity of payments increases, it becomes even more important to ensure [users] are monitoring them in near real-time.”

— SAYANTAN CHAKRABORTY, U.S. BANK

“Continual education and in-house testing of employees through mock phishing exercises to ensure that they follow proper policies and procedures can go a long way to mitigating threats,” he said.

U.S. Bank’s Menna said user training should include educating staffers about “the latest scams and schemes, and why they shouldn’t click on things.”

Companies should also have a plan in place so that employees know what to do if some sort of cyber incident does occur, she said. “How would your organization address that? How would you communicate with your customers?”

Erika Baumann, senior wholesale banking analyst at Aite Group, said she’s spoken to companies that brought in bank officials to brief their executives.

“It’s all around increased education, understanding that the bad guys are always one step ahead, and taking advantage of the information resources that are out there from the industry security experts to know what steps can be taken to better protect themselves,” Baumann said.

Given hackers’ efforts in business email compromise scams to send emails that could plausibly have come from a company executive, employees should also be “reasonably discreet” on social media, said Strategic Treasurer’s Jeffery. “You don’t need to say, ‘Here’s my boss, here’s everybody who works for me,’ so people can build the proverbial org chart,” he said.

Jeffery noted that SWIFT CSP mandates annual training for employees, and said that security is an issue for everyone. “You can’t just trust an email,” he said.

that the third party is legitimate, the bank accounts listed are legitimate.”

If payments are large, treasuries might have to have more people vet them, Seti said. “All that can be routed using workflows given the type of payment, the currency, and the magnitude of the payment.”

He also noted the “general housekeeping” that’s involved in software systems. “With most systems, you can designate, where am I putting my log files, where will my reports reside,” Seti said. “You want to be smart about where those artifacts reside. Are they in an environment that’s permissioned?”

Companies may not realize that producing a SWIFT message, for example, will result in a log entry or a backup that’s stored elsewhere on the system, he said. While the users may have forgotten about those records, hackers snooping around in the system could find them and access them if they’re not permissioned properly.

Jeffery said he sees shortfalls in treasuries’ bank account management.

“Do you have a complete inventory of all your accounts, all your signers, and all the security you have? That’s one that’s usually woefully inadequate for most organizations,” he said, adding that each bank account represents not only a cost, but also an exposure.

Companies should also have an inventory of all the payment files throughout the organization that includes where the files originated, whether they’re encrypted, and how they are transmitted to a bank or network, he said.

David Watson, global head of digital cash products for Deutsche Bank, also emphasized the importance of treasuries’ using two-factor authentication.

“If you’re not using two-factor authentication, get using it. The weakest link is people,” he said. “Any controls you can apply to the manual aspect of what you do, apply two-factor authentication. And remove as many manual steps as you can.”

Treasurers can also work to ensure that penetration testing is being done, both at their own companies and with their business partners, he said.

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