VOLUME 8 | SUMMER 2020

Cybersecurity

Designing for Privacy

Defending Against Ransomware Attacks

Learn how ransomware attacks unfold over time and how to prepare for the worst-case scenario

Verifying Vendors

How global fraud attempts have helped prompt stronger due diligence when approving vendors

Preventing Wire Fraud

Why every organization should develop strategies to help prevent and respond to wire fraud schemes

CHASE

J.P.Morgan

Cybersecurity

Designing for Privacy

So far, 2020 has brought us a world of turmoil and uncertainty, but the challenges we're all facing have brought us opportunities too. We all understand resiliency measures more deeply than before—no longer are these plans hypothetical. The enormous insight we've gained can now help us build stronger resiliency plans for whatever comes next.

Organizations can't eliminate risk. More than ever, we know the question isn't if we'll be targeted by a threat, but when. Cyber threats and fraud schemes continue to evolve, but reinforcing best practices and building strategic resiliency plans remain the foundation of a successful response.

With that in mind, our theme for this issue—Designing for Privacy—delves deeply into how organizations can adopt a culture of preparedness and strengthen awareness about privacy and security. The articles that follow can help companies like yours ask questions, look for potential vulnerabilities, and build education and training procedures to help prepare for the rest of 2020 and beyond.

In This Issue

How Organizations Design For Privacy

With innovation comes risk, so how do organizations design a framework that protects the privacy of its constituents?

The word "cybersecurity" evokes images of screens filled with binary code, fiber-optic cables spanning the globe and black-hat hackers of nefarious intent. Rarely, it seems, when we hear the word cybersecurity do we think about ethical standards.

But we live and work in an era of increased connectedness, changing business landscapes and expanded technology access at work and home. Almost everything we use on a daily basis has a "smart" version. We talk to a digital personal assistant to set the thermostat, turn on a faucet or change the channel on the TV. We drive cars that track their own maintenance and schedule their own oil changes. We use wearable tech to track our steps, sleep patterns and vital signs—and they are always on and monitoring our movements in the background. All this innovation comes with a risk: if it's connected to the internet, it may be hackable.

"This is a well-known reality for cybersecurity professionals, regardless of the particular industry they work in," said Denise Hucke, an Information Security Manager overseeing risk and controls for Commercial Banking. "The risks are real and can have financial consequences both personally and professionally."

Broadly defined, cybersecurity ethics, or cyberethics, are the complex moral dilemmas that organizations encounter in the practice and innovation of technology. They go beyond legal and regulatory requirements and ask: what is in the best interest of the public good? Cyberethics inform decisions about how to design intentionally for privacy—weighing the benefits of technological advancements against the risks to security, privacy and safety.

So how does an organization make sure their technology infrastructure and organizational culture put privacy and security at the forefront of their operations and mindset?

"It starts with asking questions," Hucke said. "You have to look at what's happening now in your organization and compare it to your code of conduct, which should include privacy and security considerations. Employees need to know they'll be supported when they pause to validate a payment change request."

Designing for Intention

As organizations adapt from traditional work environments and rely on a greater use of technology, designing for privacy is critical to help protect clients, employees and stakeholders.

Take, for example, applying artificial intelligence (AI) to generate supply chain efficiencies. The AI gathers and collates data from customer orders, supplier capabilities, weather conditions, employee staffing, and local and global shipments tracking to better predict needs or offer a more personalized experience. The technology has the potential for great good; it also has the potential for great harm by normalizing data collection. If the data is accessed illegitimately, what are the implications? Furthermore, what are the potential consequences should a state threat actor hack into the system and manipulate it to cause a service disruption or worse?

"Innovators and innovation consumers alike must delve deeply into the ethical quagmire to build a cyber ethics framework for their organizations, which accounts for these risks and stays true to their policies and culture," Hucke said.

Designing for Privacy: Questions to Ask

- What personal information (PI) do we collect and store about our clients and employees and how it is safeguarded?
- Do we have adequate controls to prevent breaches?
- How do we handle data privacy issues and unauthorized disclosures by employees?
- Do we test our security protocols periodically and regularly train all employees?
- How do we advocate for the privacy rights of our stakeholders and balance competing ethical obligations?

These are just a few questions, and they only scratch the surface of relevant considerations that executives should consider when designing for privacy. Organizations need to design for privacy keeping multiple layers and strategies in mind, such as technology builds and operational processes, and know that employees are a major access point for cybersecurity.

The challenges are deep and the implications are complex. And while the underlying ethical questions are more or less the same as throughout history, whatever ethical framework is used, the scale of potential consequences with cyber technology is historically new—and massive. Our world shares a technological fabric; pulling one thread can have unintended consequences.

> All this innovation comes with a risk: if it's connected to the internet, it may be hackable.

Ethics and Privacy in Design

Building an ethical framework for design and development.

Q/A with Denise Hucke

Q: During your 25 years working in the technology industry, you've had an inside view of how organizations handle privacy considerations. How should executives approach building an ethical framework for security within their organizations?

A: Whenever I talk to clients about cybersecurity and privacy, I stress three things: prevent, detect and respond. In our industry, we call these the three pillars of cyber hygiene. When designing systems and developing products, especially those that touch personally identifiable information (PII), the focus should be on those three pillars:

» **PREVENT:** How does the system actively prevent unauthorized access to PII? How can organizations make security protocols stronger?

Denise Hucke has been working in technology for more than 25 years, with more than 17 years in cybersecurity and controls. She is currently an Information Security Manager at the firm, overseeing risk and controls aligned to Commercial Banking. Prior to this role, she was the Business Information Security Officer and Head of Technology Controls for Corporate Technology.

Hucke is active in multiple industry consortiums and is on the Board of Advisors for the Executive Women's Forum (EWF). She has spoken at a number of events for cybersecurity leaders, including national conferences for EWF and ISC2, and she holds several industry certifications. Her mission and dedication span globally, earning her several leadership and achievement awards.

Hucke holds a master's degree in telecommunications management from Stevens Institute of Technology and a bachelor's degree in economics from Rutgers University.

» **DETECT:** What system controls are in place to detect data loss or unauthorized access, both from internal employees as well as cybercriminals, and how can organizations limit or stop it once detected?

» **RESPOND:** What processes are in place to manage threats? How do organizations learn from risk and privacy issues and build stronger controls?

This is about people. These days, our businesses and homes are filled with smart tools. These devices bring great efficiency to our lives, but as we use and design these systems, we need to consider the risks too. There has to be a balance between innovation and security.

Q: Designing an ethical framework for security goes beyond systems, but what about the human factor?

A: Culture is really important when instilling security values into your organization's ethical fabric. People are your organization's best asset. Think of them as a human firewall and train them to spot potential fraud. Make sure employees understand your values and the importance of doing the right thing at all times. Design your code of conduct and your processes to encourage questions—from all roles, whether system or product design or operational responsibilities. This is critical to protect your customers and your organization.

And make sure employees know the critical value of taking the time to validate a change in payment instructions or unusual transaction requests. When an employee makes that validation phone call to the requestor, they may stop a potential fraud attempt.

Q: What advice would you give to cybersecurity professionals?

A: Look at your organization's processes and systems—for both operations and design/development functions—to identify gaps and assess the associated risks. The list may be long so tackle the top five first, then repeat the process. Prioritization is key when weighing available resources against mitigating risks. Make sure design and development go hand in hand with the ethics of privacy.

For each piece of information your systems gather, ask, "Do we really need this?" Remember to account for the entire life cycle of the data—beginning to end. How will the data be collected, used, stored, archived and deleted?

And on an individual level, I would tell cybersecurity professionals to stay connected to professional groups. They provide a wealth of resources, support and accountability. It's in everyone's best interest to do the right thing.

> "Start with your people; they are your organization's best assets."
>
> DENISE HUCKE INFORMATION SECURITY MANAGER, COMMERCIAL BANKING

Cyber Awareness: **Clean Up Digital Clutter**

Learn how some digital cleaning can help keep your devices safe.

One afternoon, Kristen's son and his friends downloaded a free app from an unsecured, third-party website to add special effects to their selfies. The app contained malware, and when the phone was connected to her home network, the virus was able to spread to other devices, giving cybercriminals access to valuable financial data.

Email often contains sensitive information, including banking information that cybercriminals can use to commit fraud. By the time Kristen discovered several suspicious transactions on her personal accounts, the cybercriminals had already transferred the funds to another account out of the country.

Cybercriminals are using increasingly sophisticated techniques like these to access personal information. Strengthen your data and keep your devices safe with a little digital cleaning.

Getting started

Cybercriminals use malware to infect personal devices through apps and downloaded files. The first step to securing your digital presence is a good cleanse on your personal and work computers and cell phones. Encourage everyone in the family to do the same.

- Delete apps you are not using to help save space and keep your phone secure.
- Purge files from the downloads folder and recycle bin because these may contain sensitive information.
- Unsubscribe from emails and newsletters to help reduce the risk of clicking on malware or suspicious links.
- Download and archive emails you want to save; delete those you don't need—including sent items.

Protect your Devices

Use reliable protections to encrypt files and passwords, such as:

- Install a mobile security software to help keep the device secure from cybercriminals.
- Update your anti-virus software and operating system on all devices, including laptops, personal computers, tablets and phones.
- Encrypt files on laptops and PCs, so that no one can access information without your permission.

Stay Anonymous Online

Less is more when it comes to social media. Cybercriminals use what is posted, such as location, hobbies, family pictures, etc. to find potential victims and harvest personal information to try to gain access to financial accounts.

- Use separate email addresses for communication, shopping receipts and subscriptions.
- Review the privacy and security settings on your mobile devices, apps and web browsers. Limit who you share information with and confirm apps are only accessing information they need to work accurately, such as your location for mapping apps.
- Use a Virtual Private Network if you have to use public Wi-Fi while traveling to help keep your information out of the hands of cybercriminals.

Strengthen your Defenses

Here are some additional best practices to help keep your data safe:

- Only download apps from secure sites, such as the Apple App Store and Google Play. Inform your children about the dangers that rogue apps pose to the entire family.
- Use a combination of numbers, letters and special characters to create strong passwords, and consider using a reputable password manager to help manage all passwords.
- Use two-factor authentication to protect your email, social media, banking and retail accounts.
- Sign up for alerts on credit card and banking accounts to help identify potential fraudulent activity as quickly as possible.
- Put a freeze on your credit with each of the three major credit-reporting agencies to prevent cybercriminals from opening new accounts in your name.
- Verify, verify, verify. Whether it appears to be an email from a known contact or an invoice from a trusted vendor, you should remain cautious. Call the sender using a phone number from a system of record to validate authenticity.

How to Know:
Is My New Vendor Legitimate?

Organizations across the globe have mobilized extraordinary resources in response to the COVID-19 pandemic, and the resulting urgent need for medical equipment and supplies has created an opportunity for fraudsters.

Cybercriminals often use social, economic or political turmoil to escalate cyber and fraud schemes. As the health crisis has expanded globally, many organizations have needed to source medical equipment and supplies from new vendors and often have found themselves the victims of fraud attempts.

Fraudsters look for opportunities to deceive victims using social engineering attacks delivered through email, phone calls and text messages. As COVID-19 first spread, criminals continually adapted tactics to affect a wide range of organizations. Some examples include business email compromise attacks that used the health emergency as an excuse for fraudulently changing payment instructions, as well as pandemic-themed phishing emails or smishing scams that tricked victims into opening malicious attachments or links that promised information on government payments or free medical supplies.

"Criminals seize any opportunity to launch an attack and will use any means necessary, whether by email or phone," said Alec Grant, head of the fraud team with Commercial Banking. "Fraudsters are everywhere and take advantage of lapses in company best practices or security protocols."

Healthcare and government agencies were among the first industries impacted as cybercriminals escalated attacks. In March, the FBI issued a warning about the heightened potential for fraud by new vendors selling life-saving medical equipment. As the threat spread across other industries and small businesses, the tactic remained the same: scammers pretended to be new vendors claiming they could provide critical medical supplies. The criminals promised to ship supplies quickly once they received a substantial down payment. Victims made the payment, but the supplies never came and the vendors disappeared. In some cases, victims were approached by seemingly trustworthy brokers who had unknowingly worked with criminals who convinced all parties that they could deliver the needed supplies.

Now, as jurisdictions begin to lift social restrictions and stay-at-home orders, organizations are considering return to the office (RTTO) protocols, and many will need to purchase and keep on hand a stock of personal protective equipment, such as masks and gloves. As organizations implement their RTTO plans, the threat for additional fraud schemes increases not only for medical supplies, but for any purchases as fraudsters look for new opportunities to strike.

Perform and Prevent

By learning from the escalation of reported COVID-19 fraud attempts, organizations can be better prepared to adapt validation procedures to help prevent any future fraud attempts. Performing due diligence and maintaining security and authentication protocols is crucial to help stop fraud attempts. It is important to be aware of any changes in vendor information or payments, especially when responding to an urgent request.

You can help stop fraud by taking these steps:

- Remain vigilant, especially with any new vendor, and follow your organization's established due diligence procedures to approve vendor relationships.
- Know your sources. Research any potential new business partners using public databases to search names, addresses, ownership structure, tax information, articles of incorporation, business licenses and other available information to verify the validity of a company.
- Consider hiring a professional consulting firm or using paid online tools that specialize in investigations and due diligence services to assist with vendor validation.
- Review any invoices and validate any information provided, such as phone numbers and email addresses.
- Follow your accounts payable internal controls over the approval of invoices for payment and approval of the change in payment address.
- Scrutinize any email that requests a payment, changes payment instructions or changes contact information by calling the requestor directly to verify.
- Investigate any transaction that requires a full or substantial down payment before the product can be shipped. Clients should consider identifying ways to verify the supplier and goods provided.
- Review medical supply manufacturers' websites for information related to the purchase of critical supplies, such as N95 masks and other in-demand personal protective equipment.
- Report any suspicious activity involving a new vendor to the FBI.

> Staying vigilant to cyber and fraud schemes is more important than ever, and employees—whether they work remotely or in the office—should stay on guard and follow validation best practices. Remember: it only takes one person to allow—or stop—fraud.

ALEC GRANT HEAD OF CLIENT FRAUD PREVENTION, COMMERCIAL BANKING

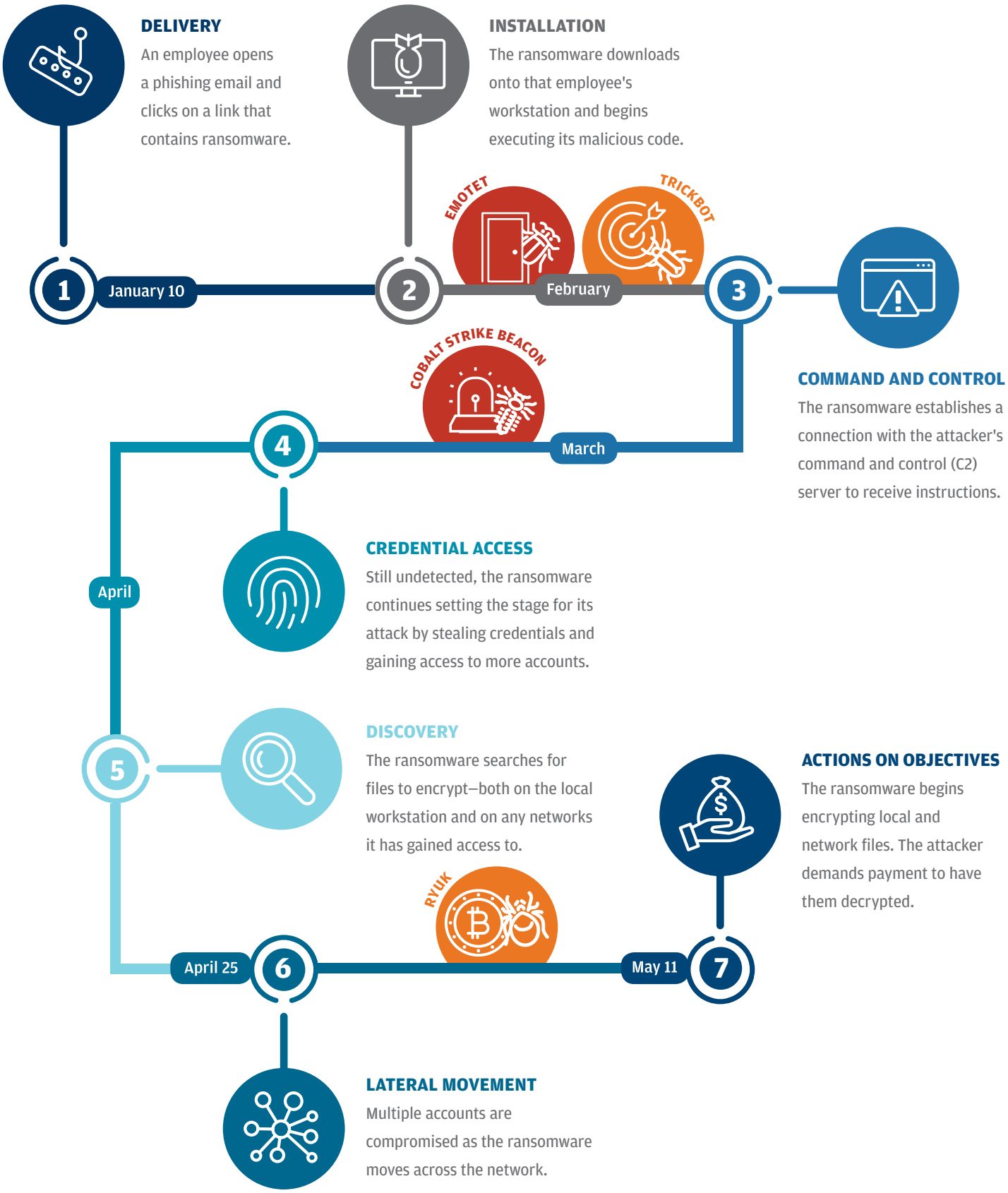
THE ANATOMY OF A RANSOMWARE ATTACK

Ransomware attacks are growing more sophisticated. Learn how they unfold and how you can prepare for the worst-case scenario.

Most businesses are probably familiar with ransomware—a type of malware that criminals use to extort organizations by encrypting and holding their data hostage until they make a digital payment.

What many may not know is that ransomware can lie undetected in an exposed organization's systems for days, weeks or even months before it's revealed through a ransom demand. Use the graphic below to follow the trail of a ransomware attack involving multiple malware strains that infiltrated an organization over the course of five months—ultimately impacting more than 11,000 servers and workstations.

The 7 Stages of Ransomware Attacks



Key: Malware Strains

EMOTET
Steals information, executes backdoor commands and delivers Ryuk payload.

TRICKBOT
Often paired with Emotet—steals login credentials and identifies targets for Ryuk ransomware.

COBALT STRIKE BEACON
Using a custom implant called "Beacon," this malware helps facilitate C2 and lateral movement.

RYUK
The final malware dropped in the attack—this ransomware encrypts systems, devices and files until a bitcoin ransom is paid.

MAZE
A new, sophisticated form of ransomware that steals private data in addition to encrypting local and network files. Criminals then threaten to release the stolen data if the ransom is not paid.

How to Ensure Your Organization Is Resilient

The best protection against ransomware is to prepare for the worst-case scenario: major disruption across the full scope of your IT infrastructure. Some steps you can take to help plan for and respond to a ransomware attack include:

- Perform a Business Impact Analysis to predict the consequences of ransomware disruption and gather information to develop recovery strategies.
- Create multiple backups to restore critical systems if the criminals delete your files (this sometimes occurs even after the ransom is paid). Ensure one set of backups is offline and inaccessible from your organization's network.
- Contact your financial institution if you are impacted by ransomware or any malware so they can be on high alert for any anomalous activity.
- Contact law enforcement including the Federal Bureau of Investigation's Internet Crime Complaint Center.
- Provide training and education for employees on how to identify and respond to suspicious emails and conduct phishing exercises.
- Contact your financial institution before attempting to pay a ransom to determine whether the financial institution can facilitate the ransom payment.
- Consider purchasing a cyber insurance policy designed to mitigate risk exposure that covers ransomware.

Why **Cyber Training** Should Matter to Your Company

Commercial Banking's Barry Rourke explains why having the right controls and maintaining continuous fraud hygiene best practices can make all the difference when it comes to protecting your company against cyberfraud.

"It's unfortunate, but true; many clients don't take the cyberfraud training we provide until after they've been the target of a cyber-enabled fraud," said Barry Rourke, a Commercial Banking relationship executive based in Bloomfield, Michigan, "and that was the case with this fraud attempt."

"Cybercriminals had spoofed one of our client's trusted vendors, forging invoices and then engaging with the client asking why the invoices were still outstanding," Rourke explained.

The scheme relied on email spoofing tactics that changed the letters in the legitimate vendor's return email address—in this case it was an "m" to an "rn." Everything else about the email matched the vendor's standard correspondences. The content of the email spelled their email address correctly and looked convincing with an accurate logo, disclaimer and signature block.

The criminals wrote that they needed to use an alternate bank account because the account of record was undergoing an audit and was temporarily unable to receive funds. "Carla," a criminal posing as the vendor's office manager, politely inquired about when payment would be sent for the invoices attached.

"Our client looked into Carla's' payment request, which was for equipment they had actually received, so they sent a payment for nearly 700,000 euros to the new account, but they didn't call the vendor on the phone using a trusted number to validate the revised banking instructions," Rourke said.

In this case, the suspicious payment was flagged by the firm's controls before the funds were sent to the beneficiary bank. Our operations team alerted the client to the validation request and escalated to Rourke, who asked the client to contact their vendor to confirm the change in account instructions. That's when the client realized the payment request was a fraud attempt; because the payment had been outsorted for client validation before the funds were released, no money was lost.

"We encourage all of our clients to complete our fraud prevention training to know how to spot suspicious emails, perform callbacks, and other red flags. Our client is extremely grateful that we called them to check the payment request stopping a potential fraud attempt, and have since improved their controls," Rourke said.

How We Can Help

You can find a variety of security measures to help protect your company from fraud, including articles and videos on our Commercial Banking Insights page. You can access this page at https://www.jpmorgan.com/commercial-banking/insights/cybersecurity.

If you have not already completed our fraud-prevention training webinars below, we encourage you to do so.

- J.P. Morgan Access® users may log on to Access and register for the Cyber Fraud & Secure Online Banking webinar via "Support > Learning Options."
- Chase Connect® users may complete the Banking and Payments Security webinar at chase.com/cybersecurity

Strengthening Global Partnerships to Help Fight Cybercrime

Effectively combatting cyber and fraud threats requires a shared commitment from government partners, public and private collaborations, and other global initiatives to help protect critical financial infrastructures. The disruptive nature of the threats, coupled with the financial impacts and data security risks, requires a dedicated strategy to share intelligence, enhance defense and resiliency protocols, and find shared solutions.

Cybersecurity resiliency is more important than ever as cybercriminals continue to evolve and expand their web of internet crimes. Eighty-one percent of companies were targets of payments fraud last year, according to the *2020 Association for Financial Professionals Payments Fraud & Control Survey Report*. Internet crime complaints are also dramatically rising. The FBI's Internet Crime Complaint Center reports that it received more than 1.7 million complaints between 2015 and 2019, reporting a loss of $10.2 billion.

Cybercriminals take advantage of chaos and uncertainty. This has been especially true during the COVID-19 pandemic. Over the last several months, threat analysts have reported an increase in ransomware attacks targeting government, healthcare and nonprofit organizations, as well as new variations of business email compromise schemes and vendor impersonation fraud attempts.

"There is no shortage of opportunity for criminals to use email, phone or social media techniques to compromise computer systems. Our fraud team has seen an elevated rate of attacks this year against clients across all sectors, and no one is immune. The need for clients to carry out greater due diligence on authentication and callback processes is more important than ever," said Alec Grant, head of the fraud team for Commercial Banking.

Cyber and fraud threats are not limited to geographic boundaries, political affiliations or select industries. Instead, criminals look for any opportunity to target vulnerabilities in a company's security and exploit cybersecurity deficiencies, often resulting in the potential exposure of personally identifiable information (PII), such as names, account information and email addresses.

"Threat actors look for weaknesses in a company's security and technology operations to try and steal data. By not maintaining tight security controls over PII, the exposure from data loss is tremendous. Personal data is a valuable commodity for criminals to sell on the dark web," said Steve Turk, Chief Data Officer for Commercial Banking.

Leading industry groups, such as the Financial Systemic Analysis & Resilience Center and the Financial Services Information Sharing and Analysis Center assist in sharing threat intelligence information and cybersecurity defense best practices.

Government agencies, such as the Department of Homeland Security and the Treasury Department, help identify monetary stressors or other risks that potentially could impact the firm and clients. JPMorgan Chase and other financial institutions work with the FBI on wire fraud cases to try to help recover stolen funds. The firm also leverages other relationships with regulators across North America, Europe and Asia to help reduce market volatility in the financial services industry and the firm's clients. For example, the Office of the Comptroller of the Currency provides enhanced awareness for the financial industry around the Small Business Administration's Paycheck Protection Program issued during the COVID-19 pandemic.

While industry members play a critical role in sharing global cyber defenses and information to help protect the financial sector, JPMorgan Chase collaborates with clients to promote awareness of the evolving threat landscape that could potentially impact their operations. Organizations can develop and maintain best practices that are specific to their needs to combat cyber and fraud threats to protect business operations, financial payment systems and personal information. A crucial part of that strategy is regular training and education for all employees, including those in the C-suite.

"Cyber threats will continue to be a part of the business landscape we live in. Clients need to be proponents of building resiliency and recovery strategies to help protect their own infrastructure, technology and critical business operations," said Mike Kelly, Head of IT Controls & Cybersecurity for Commercial Banking. "Look for vulnerabilities in your company's network and see them as opportunities to strengthen your own defenses."

Spotting and Preventing Social Engineering Attacks

Social engineering attacks have trended upward—impacting individuals and businesses. Be on the lookout for the warning signs of social engineering and learn what actions you can take to decrease the likelihood of being a victim.

Cybercriminals use social engineering to trick people into taking part in their own fraud. By posing as a legitimate business, nonprofit, government organization or other trustworthy source, fraudsters can manipulate victims into installing malware on computer systems or divulging sensitive data such as usernames and passwords, personally identifiable information and financial account information.

Social engineering attacks can spawn from practically any means of communication, but most are conducted via email, social media, phone calls or text messages. Cybercriminals often cast a wide net, targeting both individuals and businesses—no industry is immune to the threat.

What an Attack Can Look Like

Cybercriminals use times of political and economic uncertainty, especially during the COVID-19 health emergency, to escalate social engineering attacks against businesses and individuals. Some of those attacks included:

- Impersonating global health organizations in emails that contain malicious links or attachments or ask for fraudulent donations to combat COVID-19.
- Creating novel coronavirus-themed websites that distribute malware and pandemic tracking apps that contain ransomware or spyware.
- Sending emails with malicious links or attachments that offer products that are in short supply, such as other personal protective equipment.
- Conducting smishing (SMS phishing) attacks, in which cybercriminals use text messages to target victims.

How to Avoid Falling Victim

Cybercriminals also use social engineering to target employees in business email compromise scams. Consider following these best practices when validating payment requests or a change in banking instructions:

- Be extra vigilant about payments controls and validation procedures when receiving suspicious emails.
- Never click on attachments or links in emails unless you have validated the sender by hovering over the email address. When in doubt, contact your information security or technology department about any suspicious emails.
- Reconcile your bank accounts daily.
- Validate changes in all payments requests before processing by calling a known contact. Use a phone number from a system of record and follow your established internal controls. Never use the contact information provided in an email signature or invoice.
- While many employees continue to work from home, be sure to keep contact information up to date so your financial institution can contact you quickly if they detect a suspicious payment.

Finally, if you do become a victim of a social engineering attack, immediately notify your bank, file a report with ic3.gov and contact your local FBI field office to notify them of the fraud attempt.

Identifying and Responding to Wire Fraud Schemes

To prevent and respond to a wire fraud scheme, your business should not only educate all employees, but develop a comprehensive incident response plan.

Wire fraud is any fraudulent activity that occurs over interstate wire communications, including telephone lines and the internet. In many cases, the fraud attempt occurs over email. If a wire fraud payment request is not authenticated, it can result in the fraudulent transfer of money.

Cybercriminals use business email compromise (BEC) and other wire fraud methods to target payments employees. According to the FBI's Internet Crime Complaint Center, BEC caused $1.7 billion in losses in 2019 alone. On top of financial costs, businesses face potential impacts on business operations, payments systems and corporate reputation.

In addition to BEC, common methods of wire fraud include:

PHISHING, INCLUDING VOICE AND SMS PHISHING

MALWARE

Education is paramount to help prevent wire fraud. It is essential to train employees on how to spot and prevent fraud, as well as follow best practices to mitigate risk:

Establish a tiered confirmation process for new payment requests or changes in payment instructions

Never release funds if you cannot validate the request

Develop escalation protocols

Create shared protocols with third-party vendors

Implement a separation of duties between employees who request payments and those who release funds with multiple signers

Develop an Incident Response Plan

If your business experiences wire fraud, you should be prepared to respond effectively. To do so, you'll need a thorough incident response plan consisting of four stages:

1. **PREPARATION**
2. **DETECTION AND ANALYSIS**
3. **CONTAINMENT, ERADICATION AND RECOVERY**
4. **POST-INCIDENT ACTIVITY**

Reporting Wire Fraud Attempts

Victims of wire fraud should contact your financial institution to halt additional fraudulent transactions. Likewise, report the incident to law enforcement, which helps your business and others avoid similar fraud attempts.

Cyberfraud Scenario Planning

Would you know what to do if you or your employees received a suspicious email?

As the threat landscape grows across all industries, intelligence specialists say it is only a matter of time before an organization experiences a cyberattack or fraud attempt. No organization is immune from this risk.

In one type of cyberfraud attempt, fraudsters target a large corporation and use phishing attacks to compromise its email systems. After reading employee emails to learn about the company's business partners and payment processes, cybercriminals launch a pair of successful attacks.

In the first attack, the criminals use email from a look-alike domain to trick an employee into changing the payment instructions for a third-party service provider, such as the company's law firm. This action redirects payments intended for the law firm to the criminal's bank account.

In the second attack, the criminals use the compromised internal email account of an executive to send a fraudulent wire request to payments staff, who sends funds to the bank account controlled by the criminals. In both attacks, the criminals take advantage of loopholes in the organization's security and validation best practices.

If this scenario happens to your company, do you have a resiliency or fraud recovery plan to help your organization recover?

It's important for Commercial Banking clients to remember that not using the appropriate fraud-prevention tools may increase their risk of losses. Clients are liable for all losses incurred for payments originated using any authorized users' security credentials or the credentials of others who have designated transaction authority.

Do's and Don't's

Do

- Be suspicious of urgent or immediate requests to make a payment to a client or vendor, even if the request comes from an email associated with one of your company's senior managers or executives.
- Follow your company's internal controls applicable to establishing or changing a vendor's payment information in your treasury system.
- Verify new payment requests or changes in instructions received from internal employees or trusted vendors. Call the requestor directly using a phone number from a system of record, such as a company phonebook.
- Ensure there are multiple approval levels requiring signoff from different employees before submitting a payment.
- Encourage all employees to follow best practices and security protocols, including those in the C-suite.
- Regularly check all your financial accounts for any suspicious activity and reconcile bank accounts promptly.

Don't

- Skip your organization's validation procedures when you receive a change in payment instructions, a new payment request or a change in contact information, such as a phone number.
- Respond to emails without carefully examining the actual domain address before you hit send. In some cases, criminals will configure an email address to look like it came from a valid domain, but the responses will go to a look-alike domain instead.
- Click on suspicious links in emails or open attachments from unknown senders.
- Overlook the importance of regular training for all employees, including phishing exercises, and strengthening best practices for validation and verification processes.

Correction: The number of attacks against state and local municipalizes in the Fall 2019 ransomware article should be attributed to Recorded Future.

CB-MG-CYB-FL19