VOLUME 9 | FALL 2020

Cybersecurity

Assessing Risk and Securing Resiliency Strategies

Strengthening Resiliency Strategies

Assess your organizational risks in the office and at home to help bolster business resiliency and data protection measures

Fighting Payments Fraud

Understand how smaller organizations can align existing resources with additional controls to remain vigilant against payments fraud

Spotting Red Flags

Learn how one Commercial Banking client used the firm's fraud prevention education tools to prevent a $2.3 million look-alike domain scheme

CHASE

J.P.Morgan

Assessing Risk and Securing Resiliency Strategies

Cybercriminals have widened their nets and shifted tactics during the COVID-19 pandemic—taking advantage of heightened uncertainty and the vulnerabilities of working remotely. Now more than ever, organizations must remain vigilant to combat evolving business email compromise schemes, ransomware threats and data breaches that could have a severe impact on business operations and data security.

These new challenges can offer organizations a chance to take a step back and find opportunities for improvement—whether by assessing new risks, fortifying resiliency strategies, or strengthening fraud and cyber controls. Every organization, from small businesses to large corporations, can learn something new to help protect their systems, data and, most importantly, their employees and customers.

Cybersecurity is everyone's responsibility, but it starts at the top. That's why every leader should strive to ensure that their employees receive continual education and training on cybersecurity and fraud prevention best practices to help thwart and minimize these attacks. We've developed this issue—Assessing Risk and Securing Resiliency Strategies—to help start conversations and drive action on a broad range of security topics so your organization can be better prepared.

Cybersecurity

In This Issue

5 Steps to Improve Risk Assessment and Business Resiliency

JPMorgan Chase, like many organizations, applied resiliency strategies to help protect its employees, clients, processes, and infrastructure in response to COVID-19. As businesses continue to operate with a mix of in-office and remote working, you may need to engage additional resiliency strategies to avoid disruptions to business operations and services. *continued on next page >>*

Consider these five steps for future resiliency planning:

1. **Don't separate resiliency processes for on-site and remote workplaces—they're permanently connected now.** Whether your organization's current remote work environment ends with the global pandemic or continues on as a strategic option to optimize real estate and support employee flexibility, resiliency planning for systems and facilities must be ready for any scenario. Many organizations have had to adapt quickly to maintain the integrity of operations and controls in a remote work environment. These new processes may remain relevant as companies work to identify risks and weigh future changes in their physical and virtual work environments.

2. **Assume cyberattacks will continue to impact businesses at a greater frequency.** The FBI issued alerts urging organizations to increase their vigilance as fraud schemes and cyberattacks rose during COVID-19. Fraudsters may continue to seize on the potential chaos caused by the crisis and the resulting displacement of employees, vendors and customers. Maintaining your control standards and heightening employee vigilance is essential during times of disruption.

3. **Support new digital processes with greater vigilance.** When organizations were forced to adopt digital processes, cost savings and efficiencies emerged. However, data risk and cyber threats rose as well. The need to protect your data and the security of your technology infrastructure will likely grow in importance as remote work continues and new digital solutions enter the marketplace.

4. **Prepare your compliance function for cyber risks.** With the increased regulatory compliance around maintaining secure data systems, you may need to adopt robust resiliency planning strategies. Start by engaging a cross-functional team that includes legal, compliance, finance and information technology departments. This may help you evaluate ways to secure data in the event of a breach that could result in costly penalties and fines, as well as reputational harm and disruption of normal operations.

5. **Make enterprise-wide cross-training and communications planning a priority.** At many organizations, remote work and changing priorities have triggered new flexibility in roles, responsibilities and problem-solving. Constant training, testing and better communication methods have served many organizations well, and they will continue to empower workers to spot potential risks and build greater resiliency for their organizations.

Planning to bring employees back to the office?
Review this article to help get started >>

How California's New Data Privacy Regulations Could Impact Your Business

California's new landmark privacy law raises the bar for collecting and processing personal information from California consumers. Learn how this law impacts companies across different industries—regardless of where they're located.

continued on next page >>

California's comprehensive privacy law went into effect on January 1, 2020. These new requirements could have a significant impact on your business if it collects personal information about California consumers, regardless of where your business is located.

The California Consumer Privacy Act (CCPA) covers every resident in the state of California. Nearly a dozen states have introduced similar privacy bills that use all or some version of the CCPA as a template for requiring how businesses should protect consumer data.

The CCPA applies to any company based or operating in California that makes at least $25 million in annual revenue; collects data on 50,000 or more consumers, households or devices; or makes at least half of their money from selling consumers' personal information. More importantly, the CCPA includes broad definitions of consumer personal information, including predictive information on a person's behavior and identifiers such as IP addresses, geolocation and biometric data.

"We expect more states to introduce legislation that mirrors all or a significant part of the CCPA's requirements, which will change the landscape for data privacy and protection for many companies as we know it," said Steve Turk, Chief Data Officer for Commercial Banking.

California recently topped the U.K. as the world's fifth-largest economy, which means the CCPA's scope is massive given the number of companies that are either headquartered or have operations within the state—or do business with California consumers.

Many organizations want a uniform approach to data privacy regulations that includes all U.S. clients and customers rather than laws that vary state by state. However, the U.S. does not yet have a general federal consumer privacy law. As such, it's important to understand the scope and application of state privacy laws—such as the CCPA—that may impact your operations.

How the CCPA Works

Wherever your business is headquartered, if your company is subject to any of the CCPA's provisions, your California consumers have the right to request that your company disclose the personal data you keep on them. They also have the right to ask your company to stop selling that data to third-party advertisers or other entities through the "Do Not Sell My Personal Information" website link. Consumers may request to see all the personal information collected by a business and you have 45 days to disclose and deliver. Companies subject to the CCPA must provide consumers with a method for submitting these requests, which in some circumstances may be a link on the company's website.

In addition, the CCPA allows individuals to recover damages from a company that fails to maintain appropriate security procedures and practices for dealing with personal information if the company suffers a data breach.

Even if your organization currently doesn't fall under any provision of the CCPA, it's a good idea to start building compliance into your overall privacy, cybersecurity and recovery/resiliency plans, Turk said.

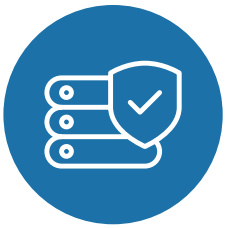
"You should know where your data is stored and protect it," Turk said. "This includes employee personal information that your human resources department would collect, such as names and Social Security numbers. It also extends to client data that you store, such as account numbers."

Turk added, "This changing regulatory environment provides both an incentive and a good opportunity to assess potential risks within all your data systems so you can prioritize actions now."

continued on next page >>

5 Ways to Manage Your Data

Maintain good cyber hygiene protocols around sensitive data, such as the principle of least privilege, which limits data access to personnel who need to know the information to perform their job function. These actions will help minimize breaches from cyberattacks, fraud attempts or employee-caused events. Your organization should also consider all relevant legal or regulatory requirements as part of this process. In addition, you should:



1. Know your data

Know exactly what client or customer data your company collects and uses.

2. Know where your data is stored

Digital and paper data storage may go through multiple iterations during the life of a business. Know how to locate it.

3. Confirm who has access

Identifying staff members with full or partial access to your data is essential for designing safer systems.

4. Limit file sharing

Investigate the latest tools to prevent file sharing, which can lead to costly data breaches.

5. Train your team

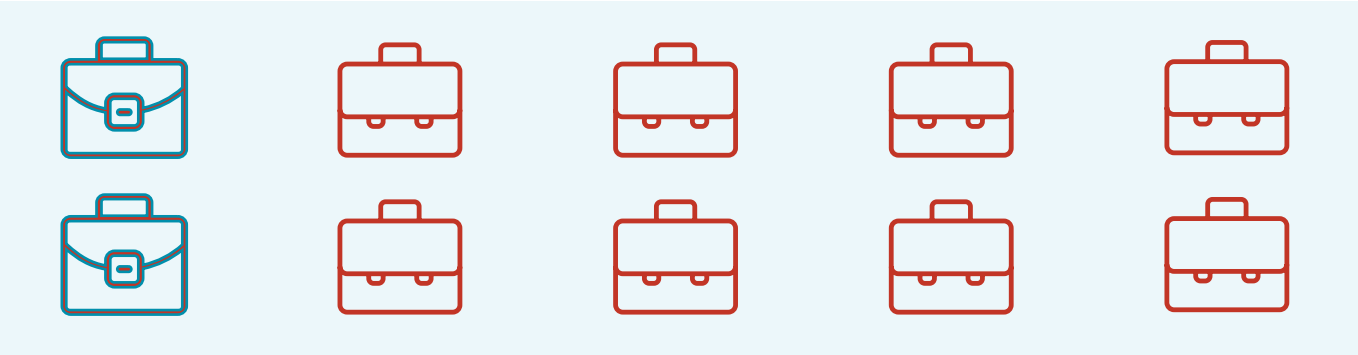
Data security begins with proper staff practices that are regularly updated and reinforced.

Security Through Simulation: How Tabletop Exercises Help Improve Incident Response

An introduction to tabletop exercises and how organizations of all sizes can begin practicing cyber preparedness.

The cyberthreat landscape is constantly evolving, with a mix of advanced nation-state actors and cybercriminals targeting organizations of all sizes. While their intentions and motivations may differ, many of their methods of attack are shared and well-publicized: social engineering, phishing, business email compromise (BEC) and ransomware, just to name a few of the most common vectors.

continued on next page >>



According to the *2020 Association for Financial Professionals Payments Fraud and Control Survey Report*, **nearly 8 in 10 organizations with annual revenue of less than $1 billion reported attempted or actual payments fraud last year.** This shows that even small and midsized businesses—that may feel constrained by personnel, time or resources to devote to cybersecurity—must remain vigilant. That's where tabletop exercises come in.

A tabletop exercise is a scenario-based discussion that's meant to simulate the various stages of a cyberattack. These exercises can play a vital role in organizational preparedness by increasing awareness of cybersecurity threats, validating response plans and procedures, and identifying capability gaps within an organization.

"Tabletop exercises are a cost-effective method that can provide a lot of value to an organization," said Adam Bulava, Global Head of Attack Simulation for JPMorgan Chase.

Tabletops bring together all the relevant stakeholders—from information technology to human resources, the sales team to the back office who may not interact much under normal circumstances.

"A crisis is never the time to exchange business cards," Bulava said.

Getting Started

A well-designed tabletop exercise can provide a low-risk environment to familiarize key personnel with roles and responsibilities, stress-test plans and foster collaboration across core functional areas of an organization.

Begin by forming an exercise planning team within your organization that will be responsible for the design, execution and evaluation of the tabletop. This team should meet regularly to determine exercise objectives, create a realistic scenario, develop supporting documentation, identify participants, manage logistics and synthesize findings for documentation in a formal after-action report (AAR).

Organizations that are new to these exercises can leverage pre-made templates and guides to help ease into the process. Email cyber.exercise@jpmchase.com for more information.

continued on next page >>

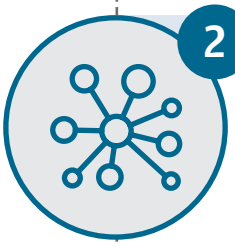
> "A crisis is never the time to exchange business cards."
>
> ADAM BULAVA, GLOBAL HEAD OF ATTACK SIMULATION FOR JPMORGAN CHASE

4 Phases of Tabletop Planning

In most cases, the lifecycle of a tabletop exercise can be broken down into these four phases:

1 Planning

In order to conduct a successful tabletop exercise, planners must obtain buy-in from leadership, develop a scenario with well-defined objectives and identify the appropriate participants.



2 Design

After laying the groundwork, planners must design the scenario used to drive the exercise and encourage active discussion across participating teams.

3 Conduct

Members of the planning team conduct a dry run and rehearse the exercise in the room or venue the day before. An exercise facilitator guides the participants through the tabletop and then conducts a "hot wash," or discussion of the exercise's strengths and weaknesses.

4 Assessment

The exercise planning team summarizes key information and findings in the AAR. The AAR should include an overview of the exercise, a list of the findings and outcomes, recommended actions for improvement, ownership and time to complete those recommended actions, and highlights from participant feedback.

Key Tabletop Exercise Objectives

- » Highlight and develop skills to lead and work through a cyber or fraud incident
- » Understand all relevant stakeholders required to respond to a significant breach
- » Learn how to conduct an exercise that could be used to test your organization's cyber preparedness
- » Take away ideas for how your organization could improve its incident response plans

What to Consider Before Purchasing Cyber Insurance

Amid the constant threat of cyberattacks, many businesses are considering cyber insurance. Would a policy be right for you?

Cybercrime has escalated in recent years, particularly ransomware. In 2019, the FBI's Internet Crime Complaint Center received 2,047 complaints of ransomware, with adjusted losses totaling over $8.9 million, according to its annual report. Business email compromise and phishing attacks have also risen as hackers use any vulnerability in validation processes or other best practices to try to gain entry into an organization's computer systems.

And the threat is more real than ever. Since the COVID-19 pandemic began, cybercriminals have picked up the pace, launching new attacks on multiple industries, including healthcare organizations, government agencies and educational institutions. They seek to disrupt business operations, steal personal data and intellectual property, and cause reputational damage.

continued on next page >>

As cybercrime has become more lucrative for hackers, organizations are considering additional resources to help protect their employees, clients and customers and cover the high costs associated with recovery. One of these options is cyber insurance. But what is cyber insurance and what does it cover?

What Is Cyber Insurance?

Insurance is a method of risk transfer that places specific risks to another person or entity for some or all of the associated financial loss. An insurance policy transfers risk through a contractual obligation from an insured to an insurance provider, subject to the terms and conditions of the insurance policy.

A cyber insurance policy provides coverage to the insured in the event of a cyberattack that results in the loss of data and/or the breach of confidential information. Depending on the terms and conditions of the cyber insurance policy, the insured could recover the cost of:

- Restoring personal identities of impacted customers
- Data restoration
- Business interruption that results in the loss of income
- Communicating to clients, customers, employees and other stakeholders
- Fines and penalties
- Security and privacy liability
- Cyber extortion
- Network interruption

Is Cyber Insurance Right for Your Organization?

Any organization that is considering cyber insurance should consult with its technology and risk departments as well as other advisors, such as an insurance broker that specializes in cyber insurance coverage. Together they should assess the risk of cyberattacks and evaluate the value an insurance policy may provide. This evaluation would include the insurance policy's deductible, premium, limit of coverage and coverage terms.

Each organization will have its own unique needs, which can include, but are not limited to: deductibles, coverage levels and insurable risks. Each of these variables can affect the final cost of insurance. It's important to keep in mind that the final cost of insurance is not merely the cost of the policy's premiums. Organizations should examine the expected value of the policy by considering the likelihood of an event occurring and the expected loss of such an event and balance those costs with insurance premiums and deductibles.

3 Guidelines to Keep in Mind:

- Determine if the maximum loss is affordable for your organization
- Consider the likelihood of losses
- Ensure that the transfer of risk is worth the premium you will pay

It's important to review the policy coverage with your insurance carrier and insurance broker to make sure your organization has appropriate coverage based on your specific needs and risk appetite. Additionally, the organization's management should also review with legal counsel the risk of a cyberattack and its impact on any regulatory or contractual requirements.

How to Stay Ahead of Fraudsters and Help Protect Your Organization

No matter the size of your organization, you can use back-end fraud prevention tools to spot suspicious fraud activity and help stop a payment loss.

Q&A with **Alec Grant**

***Alec Grant**, Head of Client Fraud Prevention for Commercial Banking, is responsible for designing and delivering strategies to protect the firm and our clients from losses. By using artificial intelligence and data analytics to detect fraud, the team seeks to enhance the client experience and increase recovery rates across all products and channels—including client education, electronic payments, check and card fraud.*

Grant has 15 years of experience building and executing fraud, financial crime and operational risk strategies. Prior to this role with the firm, he did similar work in global fraud management at Barclays and the Royal Bank of Scotland.

Grant is a sought-after industry expert who previously sat on the Global Mastercard Advisory Council, and served as chair of the Financial Fraud Trade Association. He is a former member of the U.K. Joint Fraud Task Force, chaired by the Home Secretary, and the former money laundering reporting officer of Barclays' retail bank.

Alec Grant, Head of Client Fraud Prevention, Commercial Banking, JPMorgan Chase

continued on next page >>

Q: You've spent more than 15 years working in the financial crime world. What is the biggest evolution you've seen in fraud schemes and the ways cybercriminals target organizations?

A: We are seeing an alarming increase in the number of fraud attempts against organizations. When the ***Association for Financial Professionals (AFP) Payments Fraud and Control Survey Report*** started tracking cybercrimes, 68% of organizations reported being targets of attempted or actual payments fraud attacks in 2005. Last year, 81% of organizations reported that they experienced payments fraud, according to the 2020 AFP survey report. That is the second-highest percentage reported in the past decade.

While attacks on large organizations get the headlines, it's much more likely that smaller firms with fewer resources are the most vulnerable.

Criminals are capitalizing on the changing business environment to launch new attacks against employees in the office and working remotely. During COVID-19, we saw fraudsters overwhelm smaller companies with business email compromise schemes and phishing attacks. We also saw a spike in check fraud schemes as payments employees within smaller organizations worked remotely and sent checks to pay staff and third-party vendors. Criminals are devoting significant time to finding and exploiting vulnerabilities within an organization and use the weakest link—employees—as a gateway to gain access to computer systems.

Q: What are some of the red flags to identify a potential fraud scheme, and what should clients do?

A: Criminals use a variety of tactics involving email, phone or texting to reach as many people as they can within an organization. They will also search social media profiles to find executives or employees who may have access to technology or payment systems and use that information to friend them.

Threat actors may also attempt to call employees to try and gain information on other employees, perhaps using the pretext of COVID-19 and a person's well-being. You should never accept a call from an unknown number or reveal personal information to any caller.

In a business email compromise scheme, criminals try to trick an employee to send authorized payments to an account the fraudsters control. Follow your organization's best practices to validate any changes in payment instructions or account numbers. Never email the payee to authenticate the request as you may be communicating directly with the fraudster and not the intended recipient. Too many clients email the payee to validate the request and don't realize the fraudster has already compromised the email account and is the person responding.

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

If your financial institution calls to verify a transaction, take the time to validate again with your payee directly, even if you believe the process has been done. By investing just a few minutes to authenticate the request, you could help prevent payments fraud.

continued on next page >>

Q: Fraud prevention education is necessary for all organizations, but smaller companies may have limited resources or don't know where to start. What steps can these organizations take?

A: No organization can afford to be complacent about fraud protection. The AFP survey reported that only 60% of companies have a fraud policy in place, which means that many firms learn fraud responses only after an attempt has happened.

There are back-end controls that already exist within your organization that you can implement today. Always use callback controls, back up your data and follow the principle of least privilege for payments processing to help stop fraud.

Your fraud prevention strategy should also:

Require dual payment authorization before processing any transactions

Conduct a daily spot check of less than 10% of payments to ensure that they went to the correct payee

Define and enforce your organization's escalation process for any suspicious payments requests or changes in banking instructions

Require at least two signers to approve changes to your bank accounts

Prevention is the key to avoiding fraud attempts. All employees, including C-suite executives, should follow the same controls and procedures to help maintain a strong fortress. Invest in and require regular fraud scenario training to increase awareness of fraud trends. Ensure all employees take the time to validate and raise concerns, no matter how urgent the request. It only takes one individual to give a criminal access to your computer systems.

Foiling a Look-Alike Domain Fraud Attempt

Learn how Commercial Banking's fraud prevention education helped a national university stop a $2.3 million wire fraud attempt.

Cybersecurity and fraud prevention education has played a key role in helping higher education institutions protect employees, students, alumni and vendors.

That prevention strategy helped stop a business email compromise fraud attempt for one Commercial Banking client when the criminals used a look-alike domain to impersonate one of the school's known vendors. By following the organization's established callback protocols and other best practices, the university's employees stopped a fraudulent wire transfer request for $2.3 million.

continued on next page >>

> Fraud attempts really can happen to any organization. This is the reality we live in.
>
> UNIVERSITY DIRECTOR, FINANCE AND TREASURY

Q: You learned about the fraud attempt from another university employee. What happened on that day that seemed unusual?

A: A payments employee received an email from a known vendor that requested a change to the established wire instructions and a $2.3 million transfer to a bank in Hong Kong. The employee emailed the request to the beneficiary bank and copied me. When we read the email, it sent up all kinds of red flags.

Q: What were the warning signs that this email was suspicious?

A: The email was well-written and professional, but we scrutinized it closer and noticed that the domain address from our vendor was different. There was an extra letter added to the address, so if you scanned it quickly you may have missed it. Just the day prior, we received a fraud alert from JPMorgan Chase's Fraud Prevention team about the increase in wire fraud directed to banks in Hong Kong. Our employee promptly called the vendor by phone by following our callback procedures and let them know that she had received a suspicious wire fraud request. We also learned that the cybercriminal had registered the fraudulent domain two days before attempting the wire fraud transaction.

Q: How did this fraud attempt change the university's view on cybersecurity and fraud prevention best practices, especially in the wake of expanded remote working?

A: We have shared cybersecurity emails with appropriate managers and other university members who have some level of wire authority. Going forward, we are including all wire-entitled employees on these cybersecurity alerts. We will continue to perform callbacks on new wire instructions or changed instructions on recurring payment requests that we receive.

Q: Did this fraud scheme give the university an opportunity to increase its fraud education among employees?

A: The university holds an annual cybersecurity seminar with [Commercial Banking Relationship Manager] Mike Wilson with JPMorgan Chase. Earlier this year, we expanded the distribution list to include employees from human resources, accounting, budgeting and a member of the chief investment officer's team. Moving forward, the university will increase cybersecurity presentations and include more employees from different areas. We think it is helpful for everyone to understand the pervasiveness of the different types of fraud schemes and how to spot them.

Q: What recommendations would you tell another Commercial Banking client about this experience that could potentially help them avoid a fraud attempt?

A: Fraud attempts really can happen to any organization. This is the reality we live in. Establish relationships with your vendors and pick up the phone and call them if you receive an email with a change in wire instructions and it doesn't sound right. Always do a callback.

The university's Commercial Banking Relationship team, Mike Wilson and Candice Mahanay, help reinforce the message with regular client training sessions and fraud prevention collateral.

"We regularly send cybersecurity email alerts to our Commercial Banking clients to help them stay aware of emerging cyber and fraud trends. With the rise in cybercrimes, it is important that all organizations conduct cyber and fraud education training to help educate their employees on how to spot red flags," Wilson said.

Convenience Versus Security: Avoiding Check Fraud Schemes

Checks may still be a popular payment method for many businesses, but they also may increase the risk of fraud.

Despite the efficiency and security benefits of electronic payments, checks remain a popular payment method for smaller organizations. The significant use of check payments makes it an attractive option for cybercriminals to commit fraud.

While cybercriminals have escalated business email compromise and ransomware attacks in the digital age, check fraud remains a powerful tactic because it is easy to pull off. According to the *2020 Association for Financial Professionals Payments Fraud and Control Survey Report*, 42% of business-to-business payments were made by check and 74% of organizations that used checks reported they were targets of attempted and/or actual payments fraud in 2019. ***continued on next page >>***

Criminals are opportunistic and have used the uncertainty and chaos caused by COVID-19 to launch new check fraud schemes. Payments employees working remotely may be at risk if they rely on checks as the primary vendor payment method.

"Small to midsized companies are more vulnerable to check fraud than larger organizations due to limited resources and lack of strong internal controls," said Alec Grant, Head of Client Fraud Prevention for Commercial Banking. "It's important that every organization follow a system of checks and balances for validating and authenticating payment requests prior to releasing funds."

No matter how well an organization develops security protocols, such as a dual control approval and signing process, there are multiple opportunities for a check to be stolen. After a check is initialized and printed, it should be dropped in the outgoing mail to be delivered to the payee's office. However, it can be intercepted at any point in this process. Once a criminal has the bank routing number and account number, they can create fake checks and pass them undetected between banks before they are verified.

There are additional fraud concerns that make checks more vulnerable, such as:

Forged, missing or improper endorsement

Once a check has been stolen, endorsement fraud is likely to occur and often difficult to stop. Endorsement fraud occurs when a fraudster steals a check made out to a third party, forges the endorsement on the back of the check and negotiates the check on their own behalf. If a check is payable to two parties and only one person endorses it for deposit or cash, it's considered improper unless both parties sign.

Claims that a check was deposited over a forged or missing endorsement are subject to time limits in your deposit agreement, so when a vendor calls to say they haven't received payment but, "the check is in the mail," investigate the status of the check promptly.

Internal client fraud

Guarding against internal check fraud is a concern for organizations. This type of fraud typically occurs gradually and involves multiple checks. A fraudster could be someone who works for the client, such as an assistant who has visibility into an organization's accounting practices, or a vendor who has access to checks. Working undetected, they may issue company checks to themselves or other associates to cash.

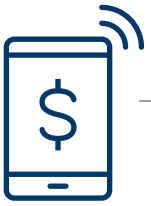
The criminal could also be an employee within the billing department who is well-trusted and handles multiple transactions. Watch for suspicious activity, such as a payments employee who doesn't take time off from work or won't accept help on payroll or other accounting tasks. Clients should conduct a random review of checks each month to ensure the check issued matches the invoice amount. Implementing a "clean desk" policy, especially among accounting or finance employees, will help secure checks and other important financial documents to guard against employee theft or a cleaning crew that serves your building.

continued on next page >>

Counterfeit checks

Criminals use technology as an advantage after stealing a check. Once a fraudster learns the organization's account and routing numbers, as well as the name and signature style of the authorized signer, they use inexpensive, high-quality printers and desktop publishing software to create convincing counterfeit checks that look legitimate. Positive Pay and Reverse Positive Pay are services that help identify and prevent payment of such items.

Mobile deposit fraud

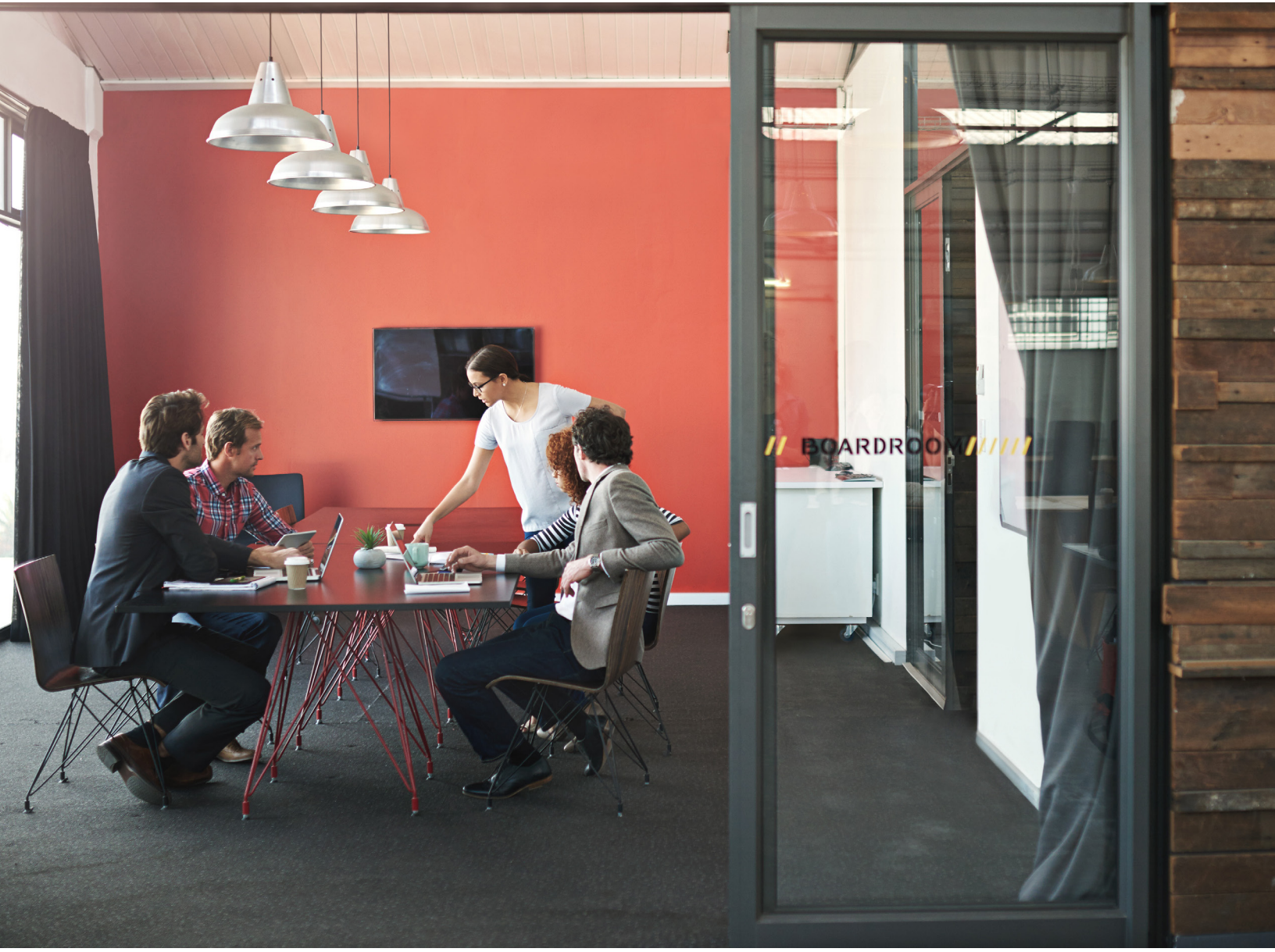


The convenience of depositing checks using mobile devices has enabled the newest—and rapidly growing—form of check fraud. In this scenario, a business issues a check to an individual who remotely captures the front and back of the check using their smartphone. After the deposit is made into their bank account, the fraudster takes the physical check to another bank or check cashing store and receives payment.

The imaged item will likely be paid by the issuer's bank, so when the paper item is presented for payment a few days later, that bank will dishonor the paper item as a suspected duplicate. The dishonored item will ultimately be returned to the party that took it from the fraudster. That party will then likely try to enforce the paper check against the company who issued it. The company's recourse will be to make a claim against its check payee, who is the fraudster, or against the fraudster's bank that took the image for deposit.

This cycle is time-consuming and expensive to resolve. It can be avoided by making electronic payments directly to payees—if they will accept payments in that fashion.

REMEMBER: Commercial Banking clients who experience check fraud are responsible for the losses that would have been preventable using available fraud protection products like Positive Pay and Reverse Positive Pay. Reconcile your check transactions daily and report any irregularities to your financial institution immediately. Contact your banking team to discuss our fraud protection services.



How Smaller Companies Can Fight Fraud with Limited Resources

Fraudsters don't discriminate based the size of a business. Take the example of one small business that fell victim to an insider payments fraud and apply the lessons learned to your own organization. ***continued on next page >>***

It's easy to feel a false sense of security in a company where everyone knows each other by name. After all, why would fraudsters try to steal from your small business when there are much bigger fish in the sea? And how could Katherine from accounting pose a potential insider threat when your kids play on the same Little League team?

The truth is, fraud doesn't discriminate based on size. Small and midsized companies are also vulnerable to schemes like business email compromise, wire fraud and insider payments fraud. One household goods importer with around 25 employees learned this the hard way. The actions it took after falling victim to insider fraud demonstrate how other companies with limited resources can combine online banking products with strong internal controls to better detect and protect against future losses.

You Think You Know Somebody ...

When the longtime president of this household goods company retired, the new leadership team began auditing financial records to identify changes or updates they could make. What they found instead was evidence that their bookkeeper, who had been working there for more than a decade, was using the corporate card for personal expenses and writing checks to herself.

The leadership team uncovered around $100,000 in fraudulent transactions going back two years. Since the company had been using paper statements and checks, this investigation process took a long time. It highlighted the need for multitouch approval controls so no one person—such as a bookkeeper—could process a transaction alone. Additionally, it revealed the need for leadership to conduct regular reviews of expense claims to validate authenticity.

Learning from a Loss

Working with their Commercial Banking team, the household goods company began reevaluating their old payments strategy. First, they moved all their accounts over to Chase Connect® with Cashflow360℠. Migrating to these digital banking platforms helped expedite processes, such as check-writing, and took much of the time-consuming workflow out of the hands of the small finance team.

In addition to simplifying their treasury management services, JPMorgan Chase provided the company tools to improve its payment approval controls. The new management team expanded their risk controls by requiring two separate individuals (including one from the management team) to digitally initiate and approve transactions. Finally, by automating their reconciliation processes, the company made sure they could quickly account for and record funds accurately. If they suspected something was awry in the future, they wouldn't have to manually pore through years of paper records again.

continued on next page >>

Best Practices to Help Protect Your Organization

Switching to digital payments solutions and using fraud protection services—as the household goods company demonstrated—can help enable faster detection of attempted fraud and better protection against future threats. But it's also very important to implement strong internal controls and best practices.

Here are a few ways to get started:

Assess Risk

- » Educate your employees about different types of payments fraud
- » Prioritize your organization's fraud risks
- » Identify accounts most susceptible to fraud and reduce the opportunity for theft

Establish Controls

- » Establish documentation requirements to support a request for a payment
- » Utilize dual controls and separation of duties to ensure oversight of all transactions and changes in vendor information
- » Perform callbacks to a vendor's number in your system of record before processing nonstandard requests for payments or changes in payment instructions or contact information
- » Identify unusual behavior through key transaction reports
- » Use fraud protection services to help minimize risk

Test Controls

- » Perform regular fraud prevention trainings to ensure controls are being used properly
- » Identify areas of weakness by conducting mock phishing emails or business email compromise (BEC) tests

The Importance of Conducting Security Due Diligence on Suppliers

Learn why organizations should review the security protocols of their third-party suppliers.

When building strong cybersecurity defenses, organizations can assess potential internal weaknesses and develop robust strategies to help mitigate risks. But even with strong internal security protocols, risks may remain if organizations do not apply the same scrutiny to the security protocols of their third-party suppliers.

The fluctuating business landscape and continued effects of the COVID-19 pandemic have amplified potential cyber risks. Small and medium-sized companies have become more dependent on suppliers as operations have shifted to remote work locations or alternate support strategies.

"Businesses needed to onboard new suppliers to maintain operations within government-mandated lockdowns," said Jim Connell, Chief Procurement Officer at JPMorgan Chase. "Some may have had urgent need for technology or critical services and may not have taken the time to conduct a thorough due diligence review. That oversight could leave an organization susceptible to a cybersecurity threat or resiliency risk."

As the threat landscape evolves and cybercriminals sharpen their attacks and fraud tactics, it's important to maintain safeguards to protect both your organization and your suppliers.

continued on next page >>

You may consider these action steps:

Develop Risk Assessment

Begin by reviewing your internal systems and processes, including every department within your organization. Apply this same assessment process to your suppliers, including any new suppliers that have been onboarded in recent months. This comprehensive control review should look for established standards and protocols to help secure any gaps, protect sensitive data from cyberattacks or fraud attempts, and establish resiliency plans in the event of a natural disaster or other emergency.

Enact Cyber Defenses Education

Conduct regular baseline employee training and perform testing exercises with key suppliers to assess the strength of existing security and identify weaknesses. If you find a lapse, require that supplier remedy it within a specific time frame.

Continue Resiliency Processes

Require every supplier to undergo a thorough evaluation, monitoring and inspection process and make any updates to secure processes. This process should continue after the relationship ends, especially if there are any regulatory or legal considerations to maintain data records for a specific period.

If you need additional resources to get started, the firm offers a variety of articles and videos on cybersecurity and fraud prevention on our Commercial Banking Insights page. You can access this page **here**.

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 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**.

If you would like to learn more about cybersecurity trends and fraud prevention, contact your banker, treasury management officer or relationship team to schedule a Commercial Banking speaker engagement session with your employees.

6 Ways to Help Protect Yourself (and Your Business) on Social Media

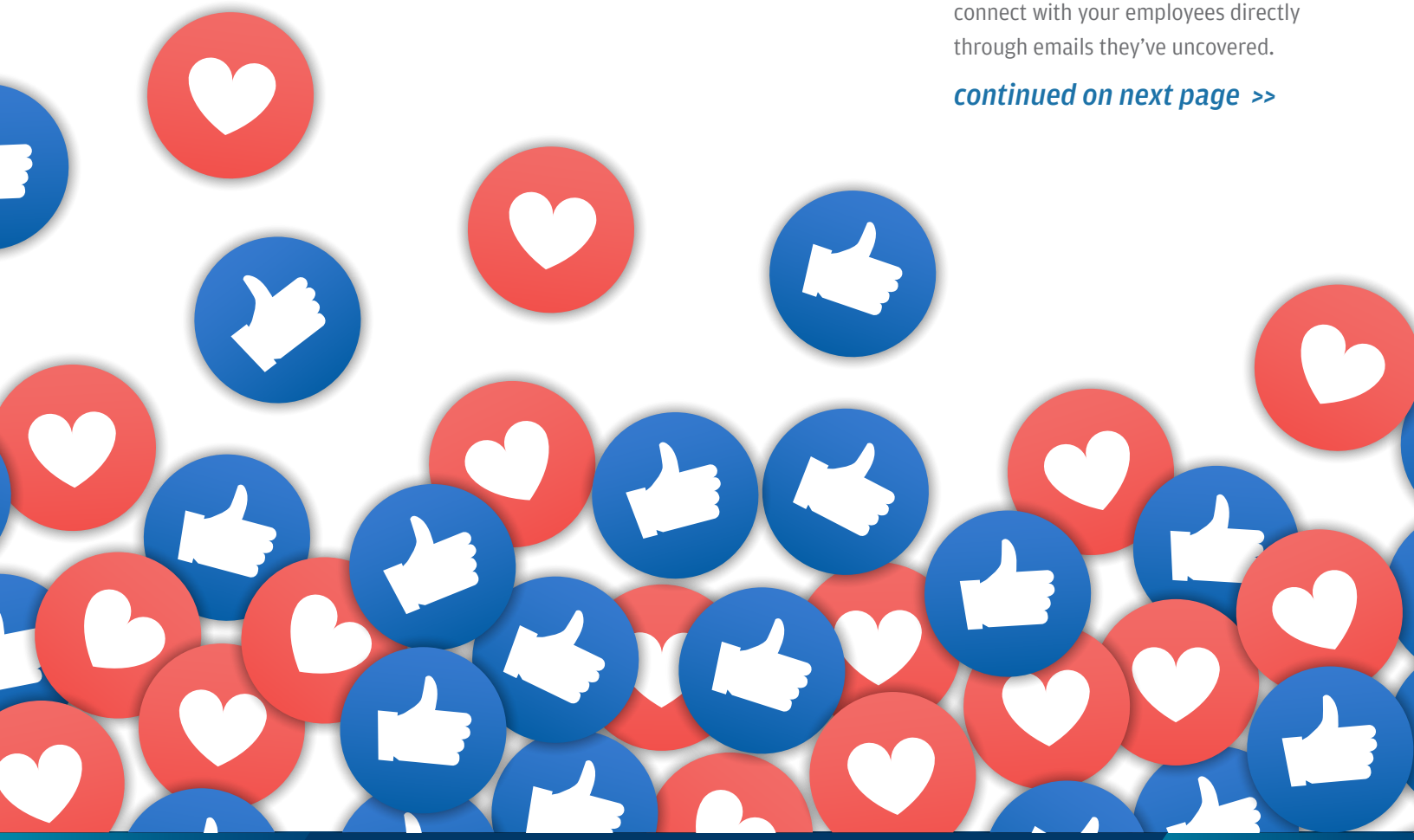
Social engineering attacks are on the rise and cybercriminals often look for clues on social media accounts. Learn how you can help protect yourself, your employees and personal information by following these six best practices using social media.

By Jonelle Burns, Head of Firmwide Cybersecurity Education and Awareness, JPMorgan Chase

You and your employees are a primary access point for cybercriminals and fraudsters on personal or professional social media. Many of the best practices and guidelines you use to protect sensitive information in the office should also apply to individuals working remotely. It only takes one person clicking a malicious email link or sharing personal information on social media to give criminals an opportunity.

Social engineering attacks often begin with social media accounts. Fraudsters may secretly investigate your organization's employee profiles, obtaining details about their work in order to piece together a believable phone conversation using this information—a practice called vishing. They may take it a step further and connect with your employees directly through emails they've uncovered.

continued on next page >>



These practices help criminals build trust with your workers and, over time, learn insider information about your company. Cybercriminals may also target your business directly—building fake employee or business profiles online, or sharing malicious links and misinformation with other users.

While the effects of a cyberattack can be long-lasting to your business operations and reputation, there are simple steps you and your employees can take to safeguard both personal and business-related information and help reduce your company's chance of being targeted.

Use privacy and security settings

Social media pages and posts are typically set to public visibility by default. Just spending a few minutes to secure your accounts can minimize your exposure and increase your security significantly.

Be strategic about connections

Only connect with people you really know and validate that it is really them. Use privacy settings to manage the amount of personal information you want to share.

Report fake profiles

Be wary of unsolicited friend requests from people you don't know. Hackers or bots use seemingly normal profiles to make connections, learn more about you or influence your decisions. Report suspicious profiles to the social media site. At work, consider investing in a process for employees to report fake profiles impersonating your brand or employees.

Avoid third-party apps and quizzes

As we spend more time working remotely, you may find social media quizzes can be a fun distraction, but at what cost? Social networks do not currently monitor the developers of quizzes, games or third-party apps for security. Also, you could be clicking on a suspicious link that shares your personal information (friend lists, email address or location) with a fraudster.

Avoid oversharing

Be cautious about how much personal and work-related information you share on your profile, posts, group chats and public pages. Even live check-ins when visiting locations can be risky. The more information you post, the easier it is for someone to identify behavioral patterns, track down your whereabouts or figure out your login credentials.

Be wary of donation scams

It's extremely common for hackers to capitalize on unpredictable events such as civil unrest, pandemics or natural disasters. Only use reputable donation sites and be mindful of crowdfunding sites to help victims after a disaster. The website may be real, but the stories posted online may be fake.

Jonelle Burns currently leads the firm's Cybersecurity Education & Awareness team, responsible for educating and empowering employees to better protect themselves, their families, and clients. Burns has more than 10 years of experience in learning and development, and has been with the firm for five years.