VOLUME 10 | SUMMER 2021

Fraud + Cybersecurity

Stay Vigilant. Stay Protected.

CHASE

J.P.Morgan

Our Commitment:

Fraud prevention is a full-team effort

Even as pandemic restrictions ease and businesses begin a return to the office, cybersecurity risks continue to intensify. Through ransomware, supply chain and social engineering attacks, cybercriminals are escalating their assaults on businesses large and small, often resulting in devastating data and fraud losses. According to the U.S. Secret Service Cyber Fraud Task Forces, current global daily losses from business email compromise schemes cost organizations approximately $8 million. No organization is immune to the risk.

Cybersecurity is not a one-time event; it is a long-term commitment to staying vigilant.

We're here to help you in that commitment. JPMorgan Chase & Co. continues to make significant investments in artificial intelligence, advanced technology and dedicated resources to mitigate risks to your finances, data and resiliency. Our Commercial Banking suite of fraud protection solutions includes cybersecurity and fraud training available on J.P. Morgan Access® and Chase Connect®.
We also offer sessions with cyber or fraud experts who can help you assess risk, implement controls and build a culture of awareness.

We encourage you to explore the insights in this issue, and engage your relationship team to discuss how they apply to your business.

Alec Grant
Head of Client Fraud Prevention for Commercial Banking

Anne Davis
Head of Cybersecurity & Technology Controls for Commercial Banking

Steve Turk
Chief Data Officer for Commercial Banking

Nick Donohue
Head of Business Continuity for Commercial Banking

Fraud + Cybersecurity

In This Issue

More than three in four companies experienced business email compromise (BEC) attacks in 2020.[1]

It's only going to become more common—criminals love BEC because it's so effective at stealing money and data. With the right controls in place, your organization can stop the scammers before they strike.

Eric Huber with Commercial Banking's Fraud Prevention Team describes how criminals research intended fraud targets to launch BEC schemes and how you can spot the warning signs.

[1] 2021 Association for Financial Professionals Payments Fraud and Controls Survey Report

Are You Prepared for a Ransomware Attack?

A road map to strengthen your organization's ransomware readiness

Ransomware and data theft continue be a major threat to government agencies and businesses, regardless of size or industry. In 2020, the FBI's Internet Crime Complaint Center (IC3) received more than 2,400 complaints identified as ransomware, costing $29.1 million in adjusted losses. Those figures don't account for lost business revenue or other operating losses to recover systems.

continued on next page >

With the availability of ransomware toolkits now on the dark web, threats to small business are increasing as novice hackers launch attacks against smaller targets.

The disruption to business operations and loss of personal information can be costly to your organization. The data loss can be far-reaching as criminals may threaten to sell stolen data, post it on the dark web or use it to attack business partners and vendors.

"We have seen a significant increase in the number of attacks against Commercial Banking clients this year," said Anne Davis, Head of Cybersecurity & Technology Controls for Commercial Banking at JPMorgan Chase. "In some cases, there are incidences of 'double extortion' style attacks where criminals issue a ransom demand for the return of stolen data then threaten to publish or share the data with competitors."

The federal government is treating ransomware as a major national security threat, and the Biden administration has called on the private sector to do its share to protect against attacks.

In a message to corporate executives and business leaders in June 2021, the White House wrote that "companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively."

To minimize losses and disruption as the result of a ransomware attack, prepare now by gathering reliable intel, documenting a response plan, testing that plan and educating employees. This road map can help you get started.

In addition to the steps outlined below, the White House recommends organizations implement multi-factor authentication, end-point detection and response, encryption, network segmentation, and prompt system patching and updating. Visit the Cybersecurity & Infrastructure Security Agency (CISA) website at cisa.gov/ransomware for more information.

Before an Attack

1 GATHER RECENT, RELEVANT AND RELIABLE INTEL.

The frequency and sophistication of ransomware attacks is increasing, so it's important to guard against ransomware attempts and understand how the attacks are carried out. Organizations must regularly gather and study current cyberthreat trends and advisories from primary sources.

Where can you get reliable threat intelligence?

- Commercial Banking's Cybersecurity and Fraud Protection Insights page
- Federal government agencies, including the Cybersecurity & Infrastructure Security Agency (CISA) and the FBI's Internet Crime Complaint Center (IC3)
- State and local agencies
- Industry partnerships such as Information Sharing and Analysis Centers (ISACs)

2 PLAN NOW, NOT LATER.

Resilient organizations anticipate the worst-case scenario and develop a cybersecurity incident response plan that engages all departments on how to respond when a real crisis strikes and causes your business to be offline for several days. The cybersecurity plan should define:

- Your payment process strategy if your organization is unable to process transactions or payroll for an extended period of time
- What priority systems or departments should be recovered first
- A data backup strategy that is aligned to your incident recovery plan
- How response teams will work to get backup systems running and operations back to normal and you have remediated the causes of the compromise

You should also test and enhance your plan regularly by conducting tabletop exercises.

continued on next page >

3 EVERYONE'S A WATCHDOG.

Your organization is only as secure as its most vulnerable points. Ransomware attacks are frequently delivered through phishing emails that appear to be sent from legitimate customers, vendors or other known contacts. But the messages contain links or attachments that, when opened, can result in your organization's sensitive data being encrypted or stolen—and in some "double extortion" schemes—both at once.

Ignoring or deleting suspicious emails in your inbox isn't enough. Here are a few steps to take and habits to reinforce:

- Require the use of multifactor authentication, like a one-time password, token or key, if a username-password combination is compromised.
- Develop, document and train employees on processes for handling suspicious emails.
- Regularly educate employees, including the C-suite, on cyber and fraud threats.
- Flag emails with an external banner to encourage staff to identify and quickly report emails that may be fraudulent to the Information Technology (IT) team before falling victim.
- Educate employees on how to spot red flags and respond appropriately throughout the various stages of a ransomware attack.

Despite your careful efforts, a ransomware attack gets past defenses and impacts your organization. What now?

During An Attack

4 REMEMBER THAT CYBERSECURITY INCIDENT RESPONSE PLAN?

When an organization is impacted by a ransomware attack, every minute is critical. Fortunately, your organization has prepared by developing and testing your incident response plan before an actual event. The IT team gets to work by identifying the source, location and extent of the attack and disconnecting infected systems. Legal, crisis communications and operations staff will need to assess when and how to inform employees, clients, stakeholders and regulators if there is a loss of data. Once the infection is contained and removed from the network, restore systems with secure, uninfected backups.

5 CONSIDERATIONS WHEN FACED WITH A RANSOMWARE PAYMENT DEMAND

- If you are the victim of a ransomware attack, you should immediately contact your local FBI field office and submit a complaint to the **FBI's IC3**.
- In assessing whether to pay a ransom demand, you should understand any regulatory and legal considerations.
- Contact your Commercial Banking relationship team as soon as you suspect a malware or ransomware incident. The team can work with you to implement protective controls on your payment platforms and assist with any resiliency needs relating to your relationship with us.

Key Takeaways

- Stay informed on the cyberthreat landscape.
- Develop an incident response plan for cybersecurity incidents, specifically ransomware attacks.
- Understand legal and regulatory considerations before considering payment of any ransom-related demand, and contact your Commercial Banking relationship team if you suspect a ransomware attack.

Are Your Vendors Cyber Ready? **10 Questions to Consider**

Even if your organization isn't directly targeted by a cyber incident, you could still feel the impacts of a supply chain attack. Here are 10 questions to consider asking your third-party vendors about their risk assessment.

continued on next page >

The widespread fallout from the supply chain attack on the information technology firm SolarWinds serves as a reminder that businesses must remain vigilant in scrutinizing the risks associated with their third-party vendors. Even if your business is not directly targeted by a supply chain attack, it could still suffer financial loss and other impacts stemming from an attack on one of your vendors.

"In a supply chain attack, criminals use your trusted vendors as gateways to gain access to your organization," said Jim Connell, Head of Global Supplier Services and Chief Procurement Officer with JPMorgan Chase & Co. "Hackers look for vulnerabilities within your vendor's network systems or manipulating the code in third-party software that are interconnected to your organization. Once cybercriminals breach those systems or applications, they can access your network."

As organizations heighten oversight and expand vendor due diligence protocols, they will need to address additional cybersecurity risks with software platforms and network systems. These considerations range from evaluating vendor preparedness to utilizing a third-party risk management service. One example, TruSight™, was founded in part by JPMorgan Chase & Co. and is designed to assess compliance by financial services industry suppliers with rigorous compliance and regulatory requirements.[1] Following a thorough evaluation and review process, TruSight scrutinizes each supplier's security practices and shares an assessment with multiple financial institutions.

Organizations should have an existing set of internal cyber controls and review existing vendor due diligence programs to ensure that they maintain your policies and procedures. If your organization doesn't have a third-party risk management program, now is the time to establish safeguards to help protect employee and client data.

What Should You Protect?

What needs to be protected varies based on your supplier relationship and the services they provide. For example, before JPMorgan Chase exchanges data with a third-party supplier, we assess their security and control environments to ensure suppliers do not introduce any unnecessary or unacceptable risk to our network.

What Is Your Liability If a Vendor Is Breached?

Liability varies based on relationship. However, if a supplier processes, stores or has access to your data, you are ultimately responsible for protecting that information. If data you own is exposed when one of your suppliers is impacted by a data breach, your organization could suffer reputational and financial impact. To address these risks in your operations, identify liability impacts and specify responsibility in your vendor contracts to protect assets and stipulate when you are alerted if a breach occurs.

Top 10 Vendor Cybersecurity Questions to Ask

Vendor risk management should look at four categories: governance, network architecture, security hygiene and incident response. Here are 10 examples of strong vendor management questions you should consider asking your suppliers to mitigate risks to your network systems:

GOVERNANCE

1. Does your vendor have a documented set of rules and procedures regulating the use of information?
2. Does your vendor have established policies and procedures for making changes to its own business processes, systems, networks and applications?

[1] TruSight's services are subject to its applicable service terms.

continued on next page >

ARCHITECTURE

3. Are there robust controls throughout your vendor's network infrastructure to help safeguard data and control access to network systems?
4. Does your vendor use encryption during the storage and transmission of sensitive data, and do they adequately protect encryption keys?
5. Is access to systems, applications and data monitored, logged and restricted to only authorized individuals with the minimal level of access necessary to complete job functions?

SECURITY HYGIENE

6. Is there a documented assessment process to identify, evaluate and report security vulnerabilities in your vendor's network, systems or applications?
7. Are there controls to detect, prevent and alert in the event of network intrusion, either as insider threats or cybercriminals?
8. Will your vendor ensure that it will keep information systems' security configurations and security patches up to date, and will they provide documentation to confirm?

INCIDENT RESPONSE

9. Is there a documented incident response plan specifically for cybersecurity and data breaches, and does the vendor periodically test it for effectiveness?
10. Can the vendor ensure timely and orderly recovery of business, support processes, operations and technology components within an agreed-upon time frame following an incident?

At a high level, there are varying courses of action to take if a vendor answers no to any of the above questions:

- For new suppliers, make sure to note in the contract that your business relationship is contingent upon remediation of high-risk control gaps. Also, consider suspending data sharing with the vendor until gaps are addressed.
- For existing suppliers, based on the severity of the gap, your organization should create an action plan that sets a timeline for remediation based on the level of risk. That includes monitoring the supplier's progress toward satisfactory performance in controls.

Above all, if a supplier is unwilling to provide information about their control environment or remediate weaknesses in it, it's probably best to find an alternate provider. Suppliers should care as much about their clients' security as their own.

Overall, trust but verify that your vendors are keeping systems secure. And if gaps are found, ensure that they are escalated and addressed quickly to protect both your business and your suppliers.

Key Takeaways

- Hackers launch supply chain attacks by identifying vulnerabilities in your vendor's computer networks or software programs to launch a cyberattack against your organization.
- Conduct a strict due diligence review of your vendor's cybersecurity protocols and require any gaps to be fixed.
- Identify liability and specify responsibility in vendor contracts if a data breach occurs.

TIP: JPMorgan Chase publishes our supplier minimum control requirements guidelines, which may be helpful to your organization when considering your vendor preparedness.

How Criminals Use Social Engineering to Target Your Company

Understand the three stages of a social engineering attack so you can build your company's defense strategy.

Cybercriminals use a variety of schemes to find vulnerabilities they can leverage to attack companies, but one of the weakest links is easier to exploit than the others: your employees.

Through social engineering—the art of manipulating people—cybercriminals study their victims, play on emotions and build trust. Attacks often create a sense of urgency or appeal toward reward, guilt or sympathy to gain access to a company's network.

"Criminals invest time and resources, such as scouring public websites and social media accounts, to study intended fraud victims," said Alec Grant, Head of Client Fraud Prevention for Commercial Banking. "Like a game of chess, these opponents gather pieces of information on victims before launching a covert attack against their defenses."

continued on next page >

The Three Stages of a Social Engineering Attack

A social engineering attack happens over three stages. The best way to protect your business from becoming a victim is to understand how attacks happen so you can implement protocols for protection. You can use the attacker's playbook to strengthen your own defense strategy.

1 Preparation

Criminals research victim by gathering public information on websites and social media. They use creative methods, such as quizzes to entice victims into providing personal information. Asking questions about cars, pets, and former schools might not seem obvious, but they provide answers to questions used to reset forgotten online account passwords.

2 Execution

The criminal uses a convincing pretext to engage the victim, build trust and gain cooperation—sometimes as simple as giving verbal information in a face-to-face conversation or getting the victim to click a file or link. Once the connection is successful, criminals can install malware into the computer system.

3 Exit

Criminals will try to conceal what's happening until they can make a proper getaway. An attack can last a few minutes, or it can progress slowly, gradually infiltrating a network before launching a ransomware attack or a payments fraud scheme. You may not realize the attack has occurred until it's too late.

Assessing Risk and Implementing Controls

With this playbook in hand, your organization can design and implement controls to prevent and detect an attack. Consider developing a social engineering prevention program to study each phase of a social engineering attack, assess your risks and build or strengthen security controls.

ASSESS RISK: **A target that's harder to scope out is a target that's harder to exploit. What information is publicly shared about your company or executives on social media, websites or in vendor profiles?**

IMPLEMENT CONTROLS:

- **Work to remove information** that can potentially be used against you in an attack.
- **Develop and enforce** a corporate social media policy to prevent disclosures about personal information, like specific job descriptions.
- **Restrict access** to websites that risk information sharing. Consider using a third-party vendor to find and remove look-alike website domains that may impersonate your company.

ASSESS RISK: **Vigilant employees are tougher to trick. How would your employees perform in a simulated test of your cybersecurity policies?**

IMPLEMENT CONTROLS:

- **Use unannounced phishing tests** to measure what proportion of employee "victims" reported receiving a suspicious email versus employees who clicked on a suspicious link.
- **Develop a continuous employee education program.** Create awareness among your staff on how to spot social engineering attacks and follow established internal policies and procedures to help protect your company.
- **Add technical controls** to flag external emails with a warning banner to make it easy for employees to report any suspicious emails.

continued on next page >

As your program matures, continuously monitor that it has the proper resources to maintain your defense protocols. Attackers are always innovating, so it's important that your plan is dynamic and ready to implement new defensive strategies.

You never know when a social engineering attack will occur. But designing a culture of preparedness now will improve your organization's resiliency and recovery efforts if you are impacted.

What Does a Social Engineering Attack Look Like?

There are several ways criminals launch social engineering attacks. Here are a few schemes to watch for:

PHISHING

Fraudulent emails that encourage you to unwittingly open harmful links or files.

SMS PHISHING (SMISHING)

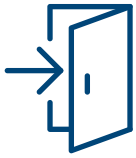
Text messages or instant messages with malicious links or files.

BUSINESS EMAIL COMPROMISE

A personalized email attack impersonating a trusted vendor or executive, often containing fraudulent payment and banking instructions.

VOICE PHISHING (VISHING)

A phone call designed to get you to share sensitive information.



TAILGATING

Also called "piggybacking." In this in-person attack, criminals seek physical access to secure areas where they can cause harm to networks.

Key Takeaways

- Know the different attack vectors criminals use.
- Look at your organization from an outsider's perspective to identify vulnerabilities or gaps that can be exploited.
- Conduct regular cybersecurity training and educate your staff on how to remain vigilant to suspicious emails, phone calls or text links.

Data Protection in a Changing Work Environment

As companies prepare to bring employees back to the office or transition to a hybrid work environment, it's a good time to review data protection practices.

The timing is right to reevaluate and adapt your data protection practices for a new dynamic workforce as companies bring employees back to the office or transition to a hybrid work environment.

When the COVID-19 lockdowns forced an abrupt restructuring to employees' routines, many organizations scrambled overnight to develop or modify controls to reduce risks. Organizations with strong data management, technology and operational response plans were able to effectively manage business demand and/or supply chain disruptions. They developed stronger security protocols, such as secure remote access, video meeting tools and enhanced data protection protocols, to ensure employees maintained compliance standards when processing sensitive information. Now, some of those temporary fixes may become permanent changes to an organization's operations and its business continuity plan.

"We've seen indicators that some data management security protocols enacted as a result of the pandemic will continue. Within Commercial Banking, our business, technology and operational support centers amplified existing design and security practices to manage data in an efficient, controlled and safe manner," said John Bassett, Executive Director for Data Management, Commercial Banking.

Take time to re-evaluate your data protection practices in the context of your new work environment. Use the questions below to assess what changes might be needed for your data privacy protocols.

continued on next page >

What's in the data, and why?

Know your data. Identify and inventory the categories and sensitivity of data that is processed by your organization. Certain data elements will require special handling and more stringent controls (for example, personal data of individuals and material non-public information). This inventory will assist in assessing requirements of specific laws or regulations about collection, use, transfer, storage, or retention of data and the impact of such requirements on the organization.

Where is the data?

Are your data, applications and services stored onsite or in the cloud? Are there backups in different locations? How readily can those backups be accessed? Do you have an incident response plan for handling scenarios, such as a cybersecurity attack that results in lost or stolen data?

You should also evaluate the security of your data in transit. Even if your server is a fortress, there's a good chance that employees may access Wi-Fi from an unsecured home network. Consider requiring encrypted connections (using a VPN or remote desktop) for all work-related tasks when connecting remotely.

Who has access, and how?

Your employees who are returning to the office may now access and print information that was under a view-only access policy during remote work. Adopt the best practice principle of least privilege, allowing authorized users access to only the specific data they need to complete their duties. Continue to remind your workforce of the need to be diligent when handling confidential data whether in paper/electronic form or being shared verbally.

Require users to create unique, complex passwords (with a combination of letters, numbers and symbols) that are changed regularly. Implement multifactor authentication, which adds additional layers of security by requiring the use of a physical token or a one-time password to authenticate the user.

Are continued investments in technology needed?

Data protection is a continuous process as new technologies, new regulations and global guidelines impact the way organizations store and share personal information. Business leaders should commit to strategic investments in new technologies that strengthen data security, such as remote security enhancements, encryption tools, data loss prevention tools, collaboration tools and metadata management.

Have you designed the right culture?

The biggest risk often isn't technology, but the humans who use it. Business leaders should develop a strong culture of data protection and safeguard practices, and stress the importance of continued cybersecurity education and training. Regular training sessions, such as lunch-and-learns or simulated drills, will help all employees understand their role in protecting data. Leaders should encourage teams to quickly report potential data risk issues and gather regular feedback from employees to help strengthen defense strategies.

Key Takeaways

- Evaluate your organization's data protection standards used during COVID-19 to enhance them for a changing work environment.
- Know your data—where it is stored, how it is used and who has access to it.
- Continuously invest in technology and data loss prevention tools.