Best Practices in Cybersecurity & Fraud Prevention

J.P.Morgan | CHASE

Disclaimer

This information is provided for discussion and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided is intended to help clients protect themselves from cyber fraud. It does not provide a comprehensive list of all types of cyber fraud activities, and it does not identify all types of cybersecurity best practices. You, your company or organization is responsible for determining how to best protect against cyber fraud activities and for selecting the cybersecurity best practices that are most appropriate to your needs. JPMorgan Chase assumes no responsibility or liability whatsoever to any person in respect of such matters. Further, the content may not be copied, published, disclosed or used, in whole or in part, for any purpose other than as expressly authorized by JPMorgan Chase.

J.P.Morgan | CHASE

Bad actors continuously seek to leverage emerging technology and vulnerabilities to carry out malicious activity…

New MOVEit Transfer zero-day mass-exploited in data theft attacks

Lawrence Abrams | BleepingComputer | 6.1.23

Hackers are actively exploiting a zero-day vulnerability in the MOVEit Transfer file transfer software, tracked as CVE-2023-34362, to steal data from organizations.

SEAN LYNGAAS CNN 07.19.2022

Russian Hackers Behind SolarWinds Breach Continue to Scour US and European Organizations for Intel, Researchers Say

A Year Later, That Brutal Log4j Vulnerability is Still Lurking

Despite mitigation, one of the worst bugs in internet history is till prevalent and being exploited

Lily Hay Newman | Wired | Dec 18, 2022

CNBC Cyber Report Elizabeth MacBride, January 9, 2023

The Dark Web's Criminal Minds See the Internet of Things as the Next Big Hacking Prize

J.P.Morgan | CHASE

This activity adds to an already-growing threat landscape that has seen increased attacks…

65%

of companies were targets of payment fraud in 2022 – down from 71% in 2021 continuing the decline from the record high 82% in 2018[1]

1.09mm

Phishing attacks sent in Q2 2022 (a new global record[2])

19%

Data breaches that were caused by a third-party in 2022[4]

45%

(highest in past 5 years) cited wires as a top payment method used in Business Email Compromise (BEC)[1]

70%

Fraudulent transactions in online banking originated from the mobile channel[3]

Note: [1] 2023 AFP Payments Fraud and Control Survey Report; [2] Phishing Activity Trends Report, Q2 2022; [3] Outseer Fraud and Payments Report H1 2022; [4] IBM Cost of a Data Breach Report 2022

J.P.Morgan | CHASE

Emerging and Persistent Threats for 2023 and Beyond

1. Malware/Zero-Days
2. Internet of Things (IoT)
3. Cloud Threats
4. Advanced Phishing
5. Quantum Computing
6. Distributed Denial of Service (DDoS)
7. Mis-Dis-Mal Information
8. Insider Threats
9. Supply-Chain attacks
10. AI/ML/Deep Fakes

How are AI/ML & Deep Fake threats evolving?

AI/ML & DEEP FAKES EXPLAINED

- Artificial Intelligence is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. [1]
- Machine learning is a subfield of artificial intelligence that gives computers the ability to learn without explicitly being programmed. [2]
- A deepfake is an image, or a video or audio recording, that has been edited using an algorithm to replace the person in the original with someone else (especially a public figure) in a way that makes it look authentic. [3]

HOW THEY'RE USED FOR CYBERCRIME

Per a 2020 Europol and Trend Micro study, "Cybercriminals have always been early adopters of the latest technology and AI is no different," when the report was published. "It is already being used for password guessing, CAPTCHA-breaking and voice cloning, and there are many more malicious innovations in the works."[4]

- Password cracking
- Adaptive malware
- Voice cloning/audio deep fake
- Video deep fake
- Large language model (ex ChatGPT) – realistic text and outputs
- Rapid malware development – "script kiddies"
- Detection Avoidance
- Break biometric security – behavior spoofing

Sources: 1. Britannica.com 2. Mitsloan.mit.edu 3. Merriam 4. Techmonitor.ai

No Industry is immune from today's cyber & fraud threats…

GOVERNMENT/EDUCATION

- **Aug 2022:** A BEC scheme involving multiple emails and criminal actors inserting themselves into communications led City of Lexington employees to send $4mm to scammers
- **May 2022:** 157-year-old college forced to permanently close due to ransomware impacting IT systems for recruitment, retention and fundraising

TECHNOLOGY

- **Jan 2023:** More than 200mm Twitter accounts, including email addresses, were leaked raising privacy and security concerns
- **Nov 2022:** T-Mobile disclosed a "bad actor" accessed personal data from 37mm current customers in a November data breach

TRANSPORTATION/TRAVEL

- **Jan 2023:** An unsecure airline database was accessed, revealing the contents of the TSA's No Fly List, containing over 1.5mm names
- **Oct 2022:** About 14 public-facing websites for several sizable airports including LaGuardia and O'Hare were brought offline by hackers

FINANCIAL

- **Dec 2022:** Hackers stole the information of nearly 35,000 PayPal users via a credential-stuffing attack on its systems in December
- **Sept 2022:** An unauthorized party gained access to an email account at Members Trust of the Southwest Federal Credit Union and may have seen the personal information of about 7,076 individuals

HEALTHCARE

- **Dec 2022:** Scripps Health in San Diego reached a $3.5mm proposed settlement to resolve a class action lawsuit stemming from a May 2021 ransomware attack and breach that impacted 2.1mm individuals
- **Jan 2022:** Maryland Department of Health was hit with a devastating ransomware attack which left hospitals struggling amid a surge of COVID-19 cases

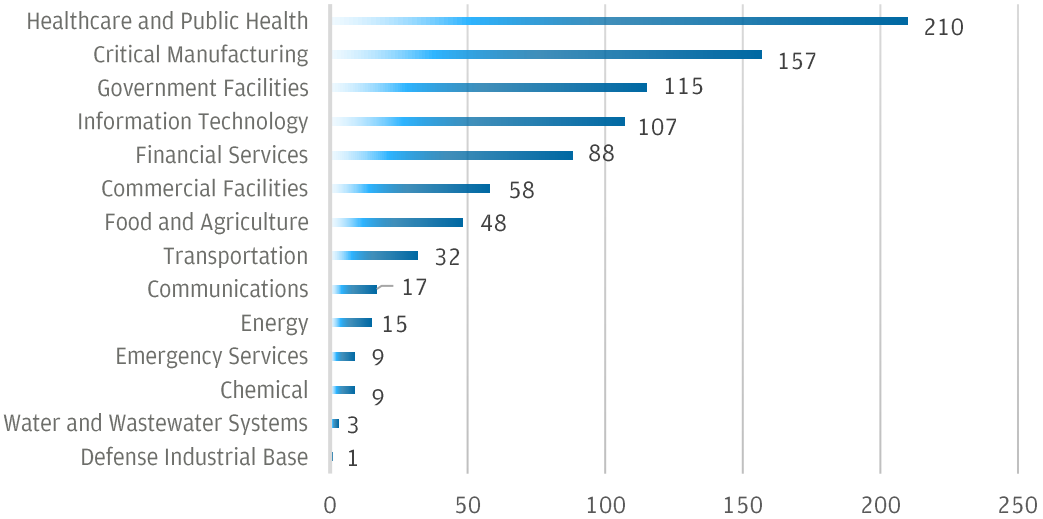
CRITICAL INFRASTRUCTURE

- **Nov 2022:** A European rail network was shut down for several hours due to possible ransomware attack on one of their sub-contractors
- **Feb 2022:** Hackers gained access to computers belonging to current and former employees at nearly two dozen major natural gas suppliers and exporters

J.P.Morgan | CHASE

Some are targeted more than others…

INFRASTRUCTURE SECTORS VICTIMIZED BY RANSOMWARE[1]



Sources: 1. FBI 2022 *Internet Crime Report (# cases reported to FBI) 2. EMSISOFT 3. Sophos*

HIGHER EDUCATION BY COMPARISON

While the FBI reported cases at left do not provide specific statistics of attacks against Education, other industry sources show:

- Per Emsisoft, 89 education sector organizations were impacted by ransomware.
- Hackers demanded ransoms from 44 universities and colleges, and 45 school districts that operate 1,981 schools[2]
- Per Sophos' annual "State of Ransomware" report based on results of a survey of 3000 IT/cybersecurity leaders across 14 countries[3]:
  - 79% of higher ed respondents were hit by ransomware in 2022[3]
  - 80% of lower ed respondents were hit by ransomware in 2022[3]
  - Across education, the majority of root causes of cyber incidents were due to either exploited vulnerabilities or compromised credentials[3]

J.P.Morgan | CHASE

Key Cyber & Fraud Risks

Business Email Compromise (BEC)

An electronic scam to obtain confidential, personal or financial information through email

Global BEC market size is expected to grow to **$3.3B** by 2028[1]

Risk Areas

- Email Spoofing / Masking
- Client Email Compromise
- Vendor Email Compromise / Supply Chain
- Lookalike Domain

Best Practice Considerations

- Consider available email security solutions to defend against lookalike domains
- Enable controls to mark outside emails as external and ensure the process for reporting suspicious emails is clear and simple
- Use call backs to confirm payment changes

Malware

Malicious software, to include viruses, ransomware, and spyware, designed to cause damage to data and systems, or gain unauthorized access

The average cost of a ransomware breach is **$4.54mm**[2] down from **$4.62mm** in 2021[3]

Risk Areas

- Malware modifying legitimate payment instructions to a bad beneficiary
- Encryption of critical files & servers for extortion

Best Practice Considerations

- Update operating systems and software
- Raise awareness about the risks of suspicious links and attachments
- Secure and monitor Remote Desktop Protocol
- Regularly backup and secure data offline

Social Engineering

Psychological manipulation of people into performing actions or divulging confidential information

19% of breaches were caused by compromised credentials and **16%** were caused by Phishing[2]

Risk Areas

- Call from someone pretending to be a vendor
- Client received SMS message from a spoofed phone number

Best Practice Considerations

- Train & test all staff regularly against the latest social engineering threats
- Limit the amount of information employees are permitted to disclose on social media
- Consider layered email controls Employee robust caller authentication processes

Sources: [1]Research and Markets BEC Report 2022, [2,3] 2022 IBM Cost of a Data Breach Report

J.P.Morgan | CHASE

Performing a Proper Callback

1 – Don't rely on inbound calls

Always conduct an outbound call to the party to confirm they are legitimate.

Never ask that a vendor call you to validate payment instructions.

Never use an inbound call to update contact information.

Why? Relying on inbound calls is an invitation for criminals to call you. If a fraudster has taken over a vendor's email, they'd know when you request that partner to call you. An outbound call from your staff to the party removes the risk that an employee falls prey to an enterprising criminal on the other end of the line.

2 – Don't trust the number provided

Always use a known or trusted number for a system of record, and continually update any internal database for improved reference ability.

Never use a phone number provided to you in an email thread, invoice or attached documentation.

Why? Fraudsters will be all too happy to validate the transaction if you call them directly. Train staff to use this system of record repeatedly, as just one deviation from the controls opens the door to fraud.

3 – Do speak with the requestor

Always speak to the party who is personally accountable for the change in instructions.

Never settle for speaking with just any employee of the vendor that's initiated a payment or change.

Why? Fraudsters with email control will exploit messages between parties. Let's say your staff calls an accounting employee at the vendor, who then emails their own CFO for validation. What your staff and the vendor don't know is that cybercriminals have hacked the CFO's email and control it. This would allow fraudsters to circumvent your controls and direct the accounting employee under the presumed guise of the executive.

4 – Don't assume internal controls have been followed

Always confirm controls were executed as intended and none of the above mistakes were made.

Never presume that a callback was performed.

Why? Human error happens; minimize its risk by actively ensuring procedures have been followed exactly as they were laid out.

Key considerations for Payments Security

User Access

- Make sure you know who has access to your banking relationships and accounts; **review entitlements regularly**
- Set **payment limits** at account and employee level based on payment trends/history (e.g., 12-month history)
- Establish **multiple approval levels** based on various thresholds (e.g., dollar amounts, tenure)
- Ensure robust and multi-level approvals required in areas such as accounts payable
- **Don't have multiple users log in from the same computer** to initiate or release payments
- Use approved templates/verified bank lines and **restrict use of free form payments**

Reconciliation

- Perform **daily reconciliation** of all payments activity – Immediate identification and escalation is critical

Verification

- **Don't move money based solely on an email or telephone instruction(s),** even from trusted vendors
- **Validate by calling** the entity requesting payment/change in instructions at their known telephone number
  - Never call a number provided via an email or pop-up
- Always **validate the sender's email address** and hover over the email address and/or hit reply and carefully examine the characters in the email address to ensure they match the exact spelling of the company domain and the spelling of the individual's name
- Never give any information to an **unexpected or unknown caller**
- **Use multi-factor authentication (MFA)** wherever possible

Detection

- **Identify** irregularities (e.g., first time beneficiaries, cross-border payments)
- **Verify** payment values and velocity
- Establish **criteria** to verify or release payments
- **Track and trace** payments to detect modification

Evolving Cyber & Fraud Risks for Merchants

Account Take Over (ATO)

Cyber criminals can take over online accounts, payment accounts, BNPL, bank accounts, etc.:

- Shipping items to a different address than billing
- IP address does not match account owner zip code
- Multiple changes to account information
- Does new PII have history of high-risk behaviour

Synthetic Identity Fraud

Occurs when a criminal creates an identity using fabricated credentials instead of stealing one:

- Often used for “new account” fraud and BNPL fraud
- Velocity checking can help spot fraudulent orders
- Device fingerprinting to check for devices previously used
- Establish manual reviews to prevent fraud and enhance customer experience

Card Not Present (CNP) Fraud

Type of fraud that does not require the physical presence of a credit or debit card, enabled by the presence of ~4.4mm cards on the Dark Web:

- Improve data collection
- Monitor for unusual behaviour
- Ask for additional authentication
- Practice good cybersecurity hygiene

Friendly Fraud

Also called first-party fraud, happens when customers dispute legitimate online purchases (i.e., chargebacks):

- Identify trends for customers that have history of chargebacks
- Have a merchant descriptor that matches the customer-facing name
- Examine store refund or exchange policy

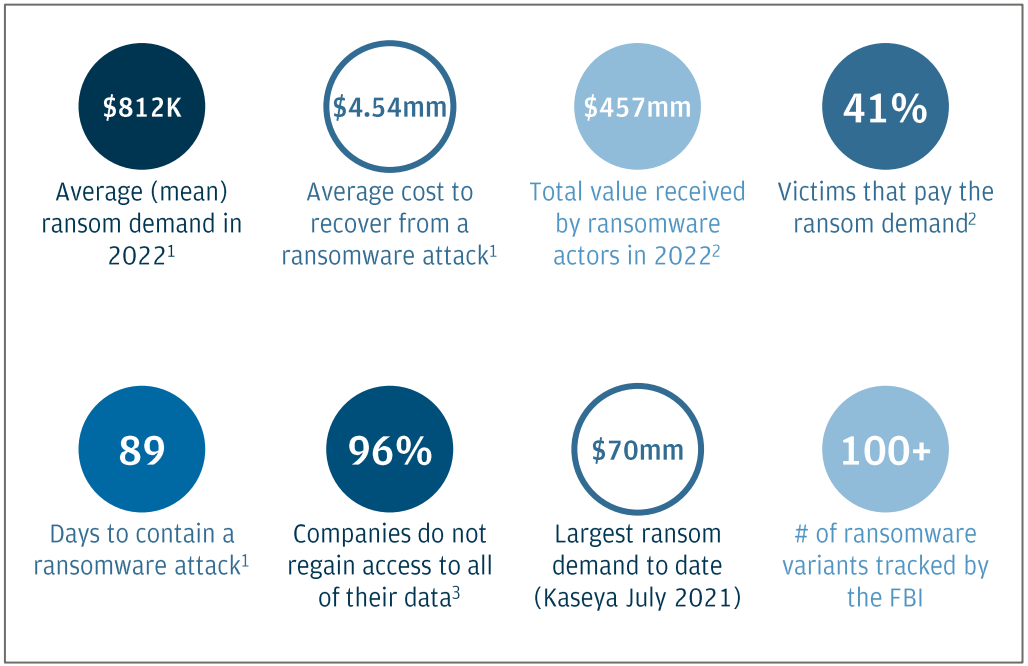
Ransomware poses an increased threat to organizations

Attacks are increasing in scale and frequency

- Ransomware operations function like a business
- 'Big Game Hunting' prioritizes high-value targets
- Ransomware-as-a-Service broadens pool of attackers
- 3,729 ransomware incidents were reported in 2021, up 37% from 2020
- In 2022, fewer companies are paying. Ransom groups have shifted more to SMBs and appear willing to take lower payouts than going after larger organizations

Paying may seem like the most attractive option

- Double and Triple extortion and other techniques increase pressure on victims to pay
- Cyber insurance has been widely adopted, but now insurers are pushing back on coverage
- Incident response takes significant time and money
- Attackers make negotiation communications and payment simple



Sources: [1]2022 IBM Cost of a Data Breach Report, [2]Chainalysis, [3]Sophos 2022 State of Ransomware Report

J.P.Morgan | CHASE

To combat these risks, employees should be reminded of the following key practices:

Enable Safe Working

Remind employees of cybersecurity **best practices** when working remotely, to include:

- Securing home Wi-Fi networks
- Only using company-approved communications tools
- Never sending work documents to personal email accounts
- Keeping personal device software up-to-date

Follow established procedures

Ensure all staff are aware of **organizational procedures** for:

- Authenticating callers
- Reporting suspicious activity
- Approving changes to account details or transactions
- Escalating potential privacy breaches

Ensure knowledge of response plans

Fully **socialize plans and playbooks** for how to escalate potential incidents and ensure clear channels for staff to alert leadership of any emerging business disruptions

Test business resiliency

Conduct regular resiliency tests and exercises to build increased preparedness among staff and ensure technology can effectively support contingency situations

“Top 10 List” of Effective Programs/Practices

- Conduct an Independent Assessment
- Engage government and law enforcement
- Join an industry forum
- Simulate an internal attack
- Deploy mandatory employee training and testing
- Know your third party vendors
- Conduct Exercises & Drills
- Understand how money leaves your organization
- Implement controls for maximum effect
- Plan for Payment Contingencies

J.P.Morgan | CHASE

Q & A

Whitepapers and webinar replays:
jpmorgan.com/commercial-banking/insights/cybersecurity