J.P.Morgan

Modernizing Your Disaster Recovery Plan

Ohio GFOA

September 2024

STRICTLY PRIVATE AND CONFIDENTIAL

Chase, J.P. Morgan, JPMorgan, and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its affiliates and subsidiaries worldwide (collectively, "JPMC", "We", "Our" or "Us", as the context may require).

We prepared these materials for discussion purposes only and for your sole and exclusive benefit. This information is confidential and proprietary to our firm and may only be used by you to evaluate the products and services described here. You may not copy, publish, disclose or use this information for any other purpose unless you receive our express authorization.

These materials do not represent an offer or commitment to provide any product or service. In preparing the information, we have relied upon, without independently verifying, the accuracy and completeness of publicly available information or information that you have provided to us. Our opinions, analyses and estimates included here reflect prevailing conditions and our views as of this date. These factors could change, and you should consider this information to be indicative, preliminary and for illustrative purposes only. This Information is provided as general market and/or economic commentary. It in no way constitutes research and should not be treated as such.

The information is not advice on legal, tax, investment, accounting, regulatory, technology or other matters. You should always consult your own financial, legal, tax, accounting, or similar advisors before entering into any agreement for our products or services. In no event shall JPMC or any of its directors, officers, employees or agents be liable for any use of, for any decision made or action taken in reliance upon or for any inaccuracies or errors in, or omissions from, the information in this material. We are not acting as your agent, fiduciary or advisor, including, without limitation, as a Municipal Advisor under the Securities and Exchange Act of 1934.

The information does not include all applicable terms or issues and is not intended as an offer or solicitation for the purchase or sale of any product or service. Our products and services are subject to applicable laws and regulations, as well as our service terms and policies. Not all products and services are available in all geographic areas or to all customers. In addition, eligibility for particular products and services is subject to satisfaction of applicable legal, tax, risk, credit and other due diligence, JPMC's "know your customer," anti-money laundering, anti-terrorism and other policies and procedures.

Products and services may be provided by banking affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those that can be provided by banking affiliates will be provided by appropriate registered broker/dealer affiliates, including J.P. Morgan Securities LLC and J.P. Morgan Institutional Investments Inc. Any securities provided or otherwise administered by such brokerage services are not deposits or other obligations of, and are not guaranteed by, any banking affiliate and are not insured by the Federal Deposit Insurance Corporation.

Changes to Interbank Offered Rates (IBORs) and other benchmark rates: Certain interest rate benchmarks are, or may in the future become, subject to ongoing international, national and other regulatory guidance, reform and proposals for reform. For more information, please consult: https://www.jpmorgan.com/IBOR

JPMorgan Chase Bank, N.A. Member FDIC. Deposits held in non-U.S. branches are not FDIC insured.

© 2024 JPMorgan Chase & Co. All rights reserved.

Unraveling the impact of ecological or economic challenges

Hurricanes

Pandemic

Wildfires

Floods

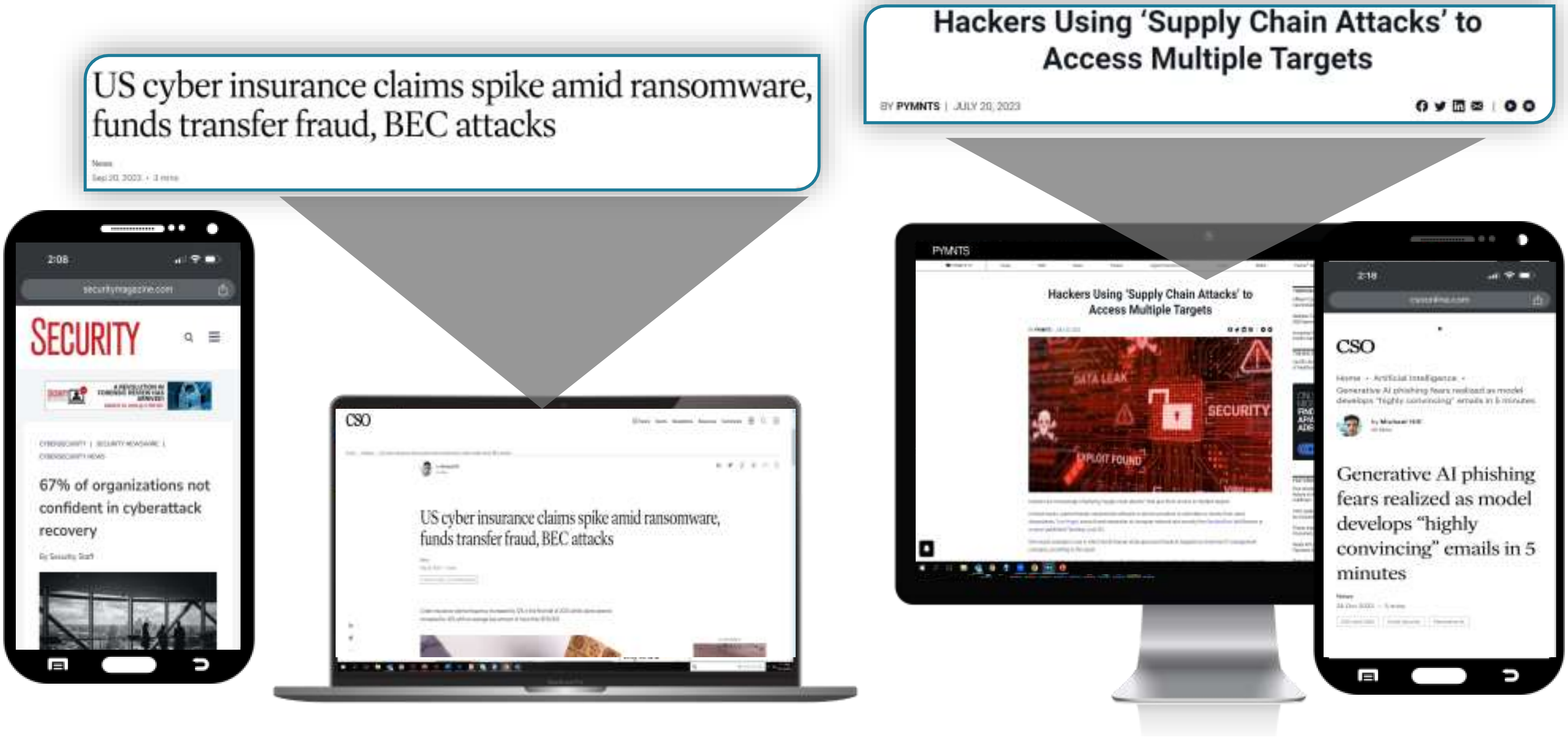
Chaos opens the door for bad actors

Financial Crisis

Facility Destructions

Cyber Attack

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



US cyber insurance claims spike amid ransomware, funds transfer fraud, BEC attacks

News
Sep 20, 2023 • 3 mins

Hackers Using 'Supply Chain Attacks' to Access Multiple Targets

BY PYMNTS | JULY 20, 2023

SECURITY

67% of organizations not confident in cyberattack recovery

By Security Staff

CSO

US cyber insurance claims spike amid ransomware, funds transfer fraud, BEC attacks

PYMNTS

Hackers Using 'Supply Chain Attacks' to Access Multiple Targets

CSO

Generative AI phishing fears realized as model develops "highly convincing" emails in 5 minutes

Security Magazine article; CSO Online article; PYMNTS article; CSO Online article

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

1,265%

Increase in phishing attacks since the launch of ChatGPT in Nov 2022[1]

70%

Percentage of organizations that distrust their current internal controls to prevent payment fraud[2]

88%

Percentage of respondents surveyed by the Ponemon Institute that reported being a victim of payment fraud during the years 2022 and 2023[2]

59%

Companies that experienced a data breach due to a 3rd Party[3]

49%

Percentage of companies that do not have proper insurance to cover transaction fraud, even after experiencing fraud[2]

[1] SlashNext 2023 State of Phishing Report; [2] Ponemon Financial Security Trends '23 ; [3] State of Cybersecurity and 3rd Party Remote Access Risk

No industry is immune from today’s cyber & fraud

SOCIAL MEDIA/ DIGITAL CURRENCY

Mar 2022: Hackers stole nearly $600MM in cryptocurrency from a crypto sidechain project by accessing private keys and forging fake withdrawals

Aug 2023: A widespread hijacking campaign was executed on LinkedIn accounts, locking users out or threatening deletion unless a ransom is paid

NBC News article; Bleeping Computer article

FINANCIAL SECTOR

June 2023: The European Investment Bank experienced severe website outages due to a cyber attack carried out by Russian threat actors

May 2023: Several banks were breached due to the MOVEit vulnerability, exposing customer and/or employee information

BankInfoSecurity article; American Banker article

TECHNOLOGY SERVICES

Feb 2022: A leading Australian SaaS company halted trading after discovering unauthorized activity in their systems

May 2023: An American Telecom company disclosed a data breach that compromised the personal information of 37MM people

Reuters article; Forbes article

HEALTHCARE & PUBLICH HEALTH

Aug 2023: A California- based healthcare provider was affected by ransomware, causing emergency room shutdowns in multiple states

Oct 2022: A Ransomware attack affecting one of the largest U.S. hospital chains caused delays in surgeries and patient care at the over 140 hospitals

NBC News article; The New York Times article

TRAVEL/ TRANSPORTATION

July 2023: Japan’s largest port was temporarily shut down as a result of a ransomware attack

May 2023: A Scandinavian airline was attacked by Anonymous Sudan, causing website and application outages for nearly an entire day

Bleeping Computer article; The Record article

CRITICAL INFRASTRUCTURE

Feb 2022: Hackers gained access to current and former employees’ computers at nearly two dozen major natural gas suppliers and exporters

Jul 2023: Chinese state sponsored threat actors gained persistence in US military infrastructure, representing a serious threat in the event of future crises

Bloomberg article; Dark Reading article

Top 10 Cyber Attacks

Drive-by Attacks/Cross Site Scripting

Malware/Ransomware

External Remote Services Exploitation

Phishing Attacks/Social Engineering

Public Facing Application / Vulnerability Exploitation

Distributed Denial-of-Service (DDoS) Attacks

SQL Injection

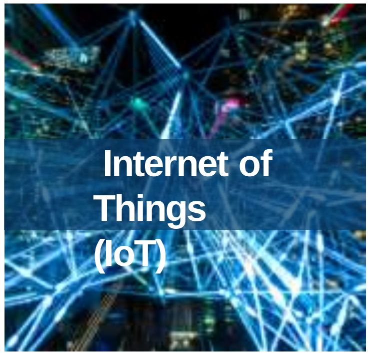
Weak Passwords/Password Attacks

Supply Chain Attacks

Man-in-the-Middle Attacks

Emerging and Persistent Threats for 2023 and Beyond

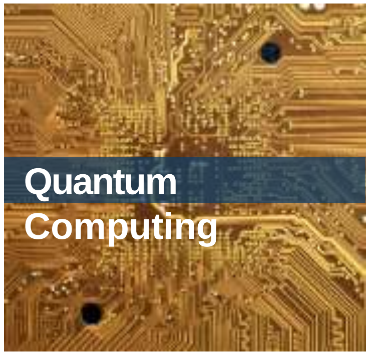
Malware/Zero-Days



Internet of Things (IoT)

Cloud Threats

Advanced Phishing



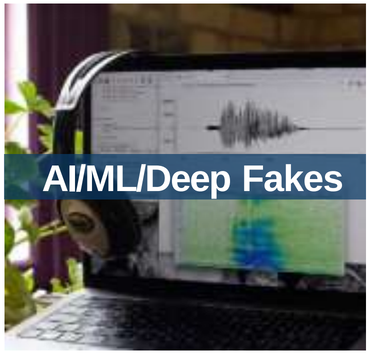
Quantum Computing

Distributed Denial of Service (DDoS)

Mis-Dis-Mal Information

Insider Threats

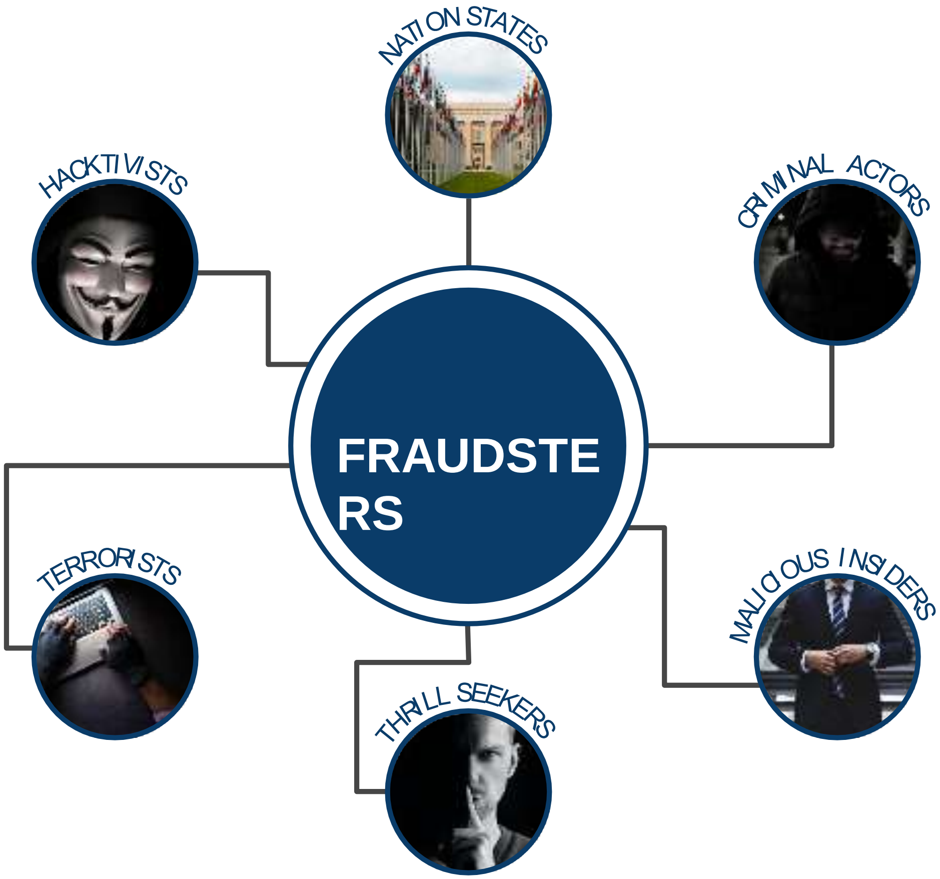
Supply-Chain Attacks



AI/ML/Deep Fakes

Who Commits Fraud?

- Not all fraudsters are the same. Some are criminals or part of criminal organizations that are motivated by money and self-interest
- Some fraudsters are motivated by revenge and a desire to get back at agencies for perceived offenses
- Other fraud actors are part of nation-states or terrorist groups that conduct attacks to enrich their home country or to harm the victim country
- Other actors may be motivated by the thrill of conducting illegal activity or by seeing what they can get away with



Common Payment Fraud Scenarios

Vendor & Executive Impersonation

Impersonation tactics used to deceive organizations into fraudulent payments. Business Email Compromise is a common tactic

Third-Party Compromise

Occurs when an organization's vendor or supplier is hacked leading to the manipulation of billing details or bank accounts, resulting in fraudulent transactions

Account Takeover

When an attacker gains unauthorized access to a corporate bank account, often using stolen or compromised credentials to make unauthorized transactions

Malicious Insider/User Entitlement Fraud

Intentional actions by current or former employees or contractors, contractors, where they gain access access to accounts to manipulate manipulate payments

Systems and Human Error

Although not fraud, these unintentional errors can cause financial losses. This includes instances where someone inputs incorrect payment information

Sanctioned Entities

Payments made to sanctioned entities, resulting in potential legal repercussions, financial losses, and reputational damage

AI is being leveraged by threat actors to aid their social engineering capabilities…

Sophistication

- More convincing and formal wording
- No more language barrier
- Undermines historical indications of phishing/scams (misspelled words, poor grammar, etc.)
- Greater accessibility and a lower barrier of entry

Deepfake

- Video, audio, and photo deepfake technologies are improving rapidly
- Real-time capabilities for impersonation
- Bypassing remote identity verification systems such as facial recognition or voice authentication

Automation

- Can be used for phishing, misinformation, & social media campaigns
- Increases efficiency for attackers and allows for higher volume attacks
- Intelligence gathering using data mining across different platforms (social media, public records, etc.)

Key considerations for payment 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
- Make sure **multiple users do not log in from the same computer** to initiate or release payments
- Use approved templates/verified bank lines and **restrict use of free form payments**

Verification

- Make sure **money is not moved based solely on an email or telephone instruction(s),** even from trusted vendors
- Try to **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 carefully examine the characters in 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

Reconciliation

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

Detection

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

To combat these risks, follow 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 Response Plan Awareness

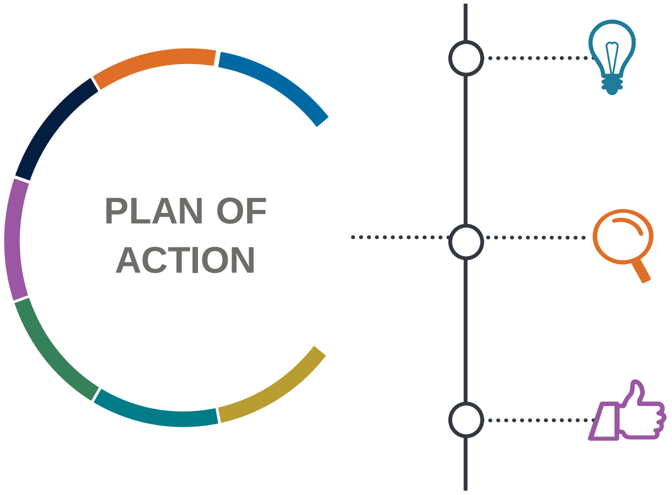
Fully **socialize plans and playbooks** for how to escalate potential incidents and ensure clear channels for staff to alert leadership of any emerging business disruptions

Test Business Resiliency

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

Business Continuity Planning (BCP) for Resilience

Establishing an effective technology and system continuity plan to limit losses and quickly stand back up the organization during a disruptive event



PLAN OF ACTION

Pre-Crisis

It is important to establish a BCP pre-crisis to create a set of strategies and preventative action plans to ensure full functionality of essential services in a disaster recovery scenario

During Crisis

Deploy BCP and conduct testing of systems and technology periodically to validate the applicability and performance of your plan

Post-Crisis

Conduct a review post crisis to incorporate any lessons learned or feedback from employees to improve the plan for the next event

What J.P. Morgan can do for you?

- Provide best practices and guidelines to identify opportunities to improve your technology BCP
- Offer insights to assist with your technology implementation roadmap
- Based on best practices, help you develop a playbook to review system entitlements
- Create and rollout strategy to provide a full suite of electronic payment and collection services, which can operate even if mail or physical facilities are disrupted
- Propose thought leadership and scorecards to help with other areas of business resiliency

“Top 10 List” of effective programs/practices

Conduct an independent assessment

Engage government and law enforcement

Conduct exercises & drills

Understand how money leaves your organization

Join an industry forum

Simulate an internal attack

Implement controls for maximum effect

Plan for and test payment contingencies

Deploy mandatory employee training and testing

Know your third-party vendors

QUESTIONS

????