Modern Disaster Recovery & AI-Driven Threats

Ohio GFOA | September 2025

JPMorganChase

Speaker Highlight

Candice Biamby

Vice President, JPMorganChase

Candice Biamby is a Vice President in Cyber Threat Intelligence at JPMorgan Chase, specializing in incident response, incident readiness, and endpoint security, with a strong track record of enhancing cybersecurity across a variety of organizations.

Carol Ellis

Vice President, JPMorganChase

Carol brings over 40 years of banking experience, including 17 years in treasury management, specializing in government banking. Her responsibilities include recommending cash flow optimization strategies, streamlining financial processes, and providing insights on new products and market trends.

Greg Mullins

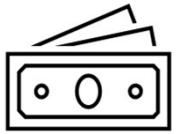
Vice President, JPMorganChase

Greg is the Vice President in Government Banking at J.P. Morgan focusing on introducing innovative treasury services and financing strategies to large government clients in Kentucky, Southwest Ohio, and West Virginia. With 34 years in banking, Greg has served in various roles across Retail Banking, Credit, Commercial Real Estate, and Commercial Banking.

Agenda

- Why This Matters Now
- The Modern Cyber Threat Landscape
- The AI Acceleration Factor
- Fraud & Attack Prevention
- Building Resilience in an AI-Drive Threat Era
- Closing

The New Reality of Cyber Threats

$10.5T 

Expected cost of global cybercrime annually by 2025[1]

60% 

Of participants fell victim to AI-generated phishing emails, a rate comparable to non-AI phishing crafted by experts[2]

42% 

Of all detected fraud attempts in the financial and payments sector involved AI[3]

AI is reshaping the threat landscape—attackers are faster, smarter, and harder to detect

[1] https://cybersecurityventures.com/cyberwarfare-report-intrusion/
[2] https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams
[3] https://www.rfidjournal.com/news/ai-fraud-attempts-with-deepfakes-spike-in-last-three-years-signicat/223028/

Slide 4

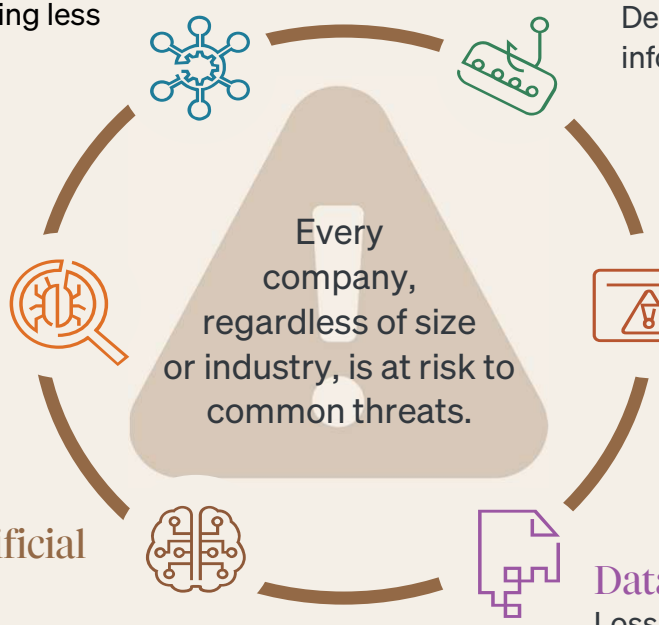
ECA(U0 As we discuss Modernizing your disaster recovery plan, we are going to talk a lot about AI threats. As we all know AI is truly shaping the threat of how attackers are doing business. Hackers are becoming faster, smarter and harder to detect. I

Ellis, Carol A (CCB, USA), 2025-08-27T14:32:23.496

The Modern Cyber Threat Landscape

Supply Chain Compromise
Compromising an organization by targeting less secure partners of its supply chain

Social Engineering
Deceiving individuals into revealing sensitive information or obtaining unauthorized access



Ransomware and Malware
Malicious software designed to block access or encrypt data until a ransom is paid

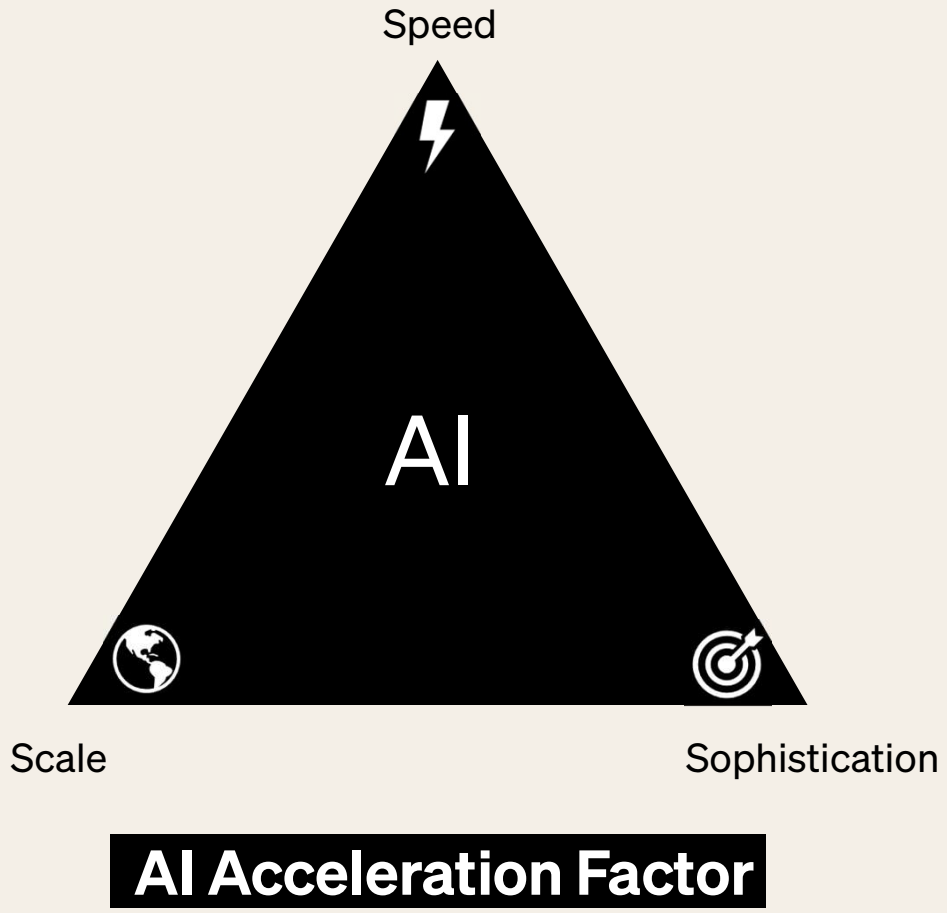
Distributed Denial of Serivce (DDoS)
Disrupt availability of services with flood of malicious Internet traffic

Disinformation and Artificial Intelligence (AI) Abuse
Improper use of AI and synthetic media to deceive end users and perpetrate fraud

Data Loss and Breaches
Loss of confidential information from both internal and external threats

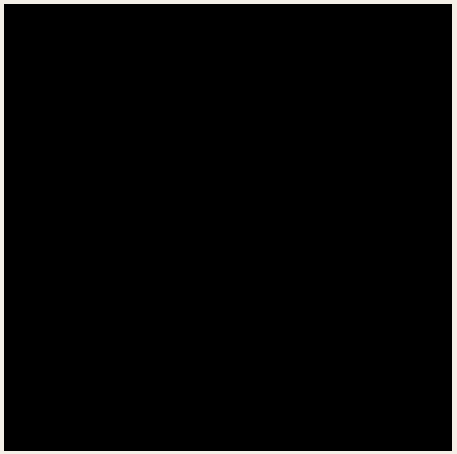
Why AI changes the game

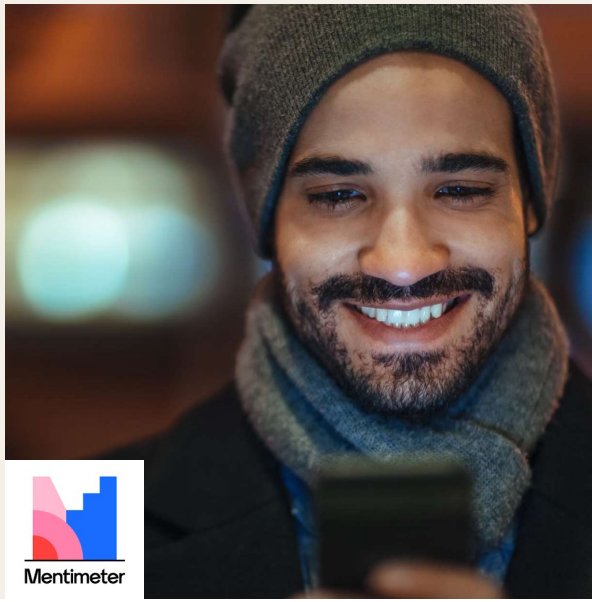
- 2x more phishing attempts use AI
- 3x faster credential stuffing with AI automation
- Attackers gain:
  - Speed
  - Scale
  - Sophistication



Test your knowledge – checkpoint #1

Ready to test your cyber knowledge?
Scan the QR code below or go to
menti.com and use code: 1363 8053 BC(U0



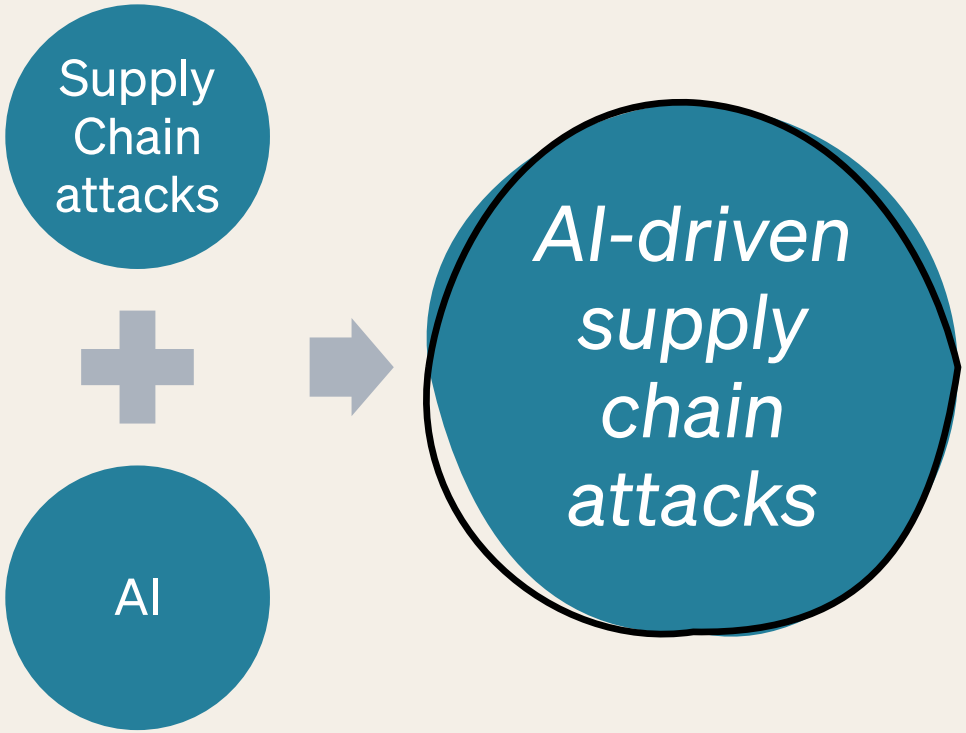


Slide 7

BC(U0 Note to self: update with code before presentation as it will expire on 9/5

Biamby, Candice (CTC, USA), 2025-09-04T03:34:03.922

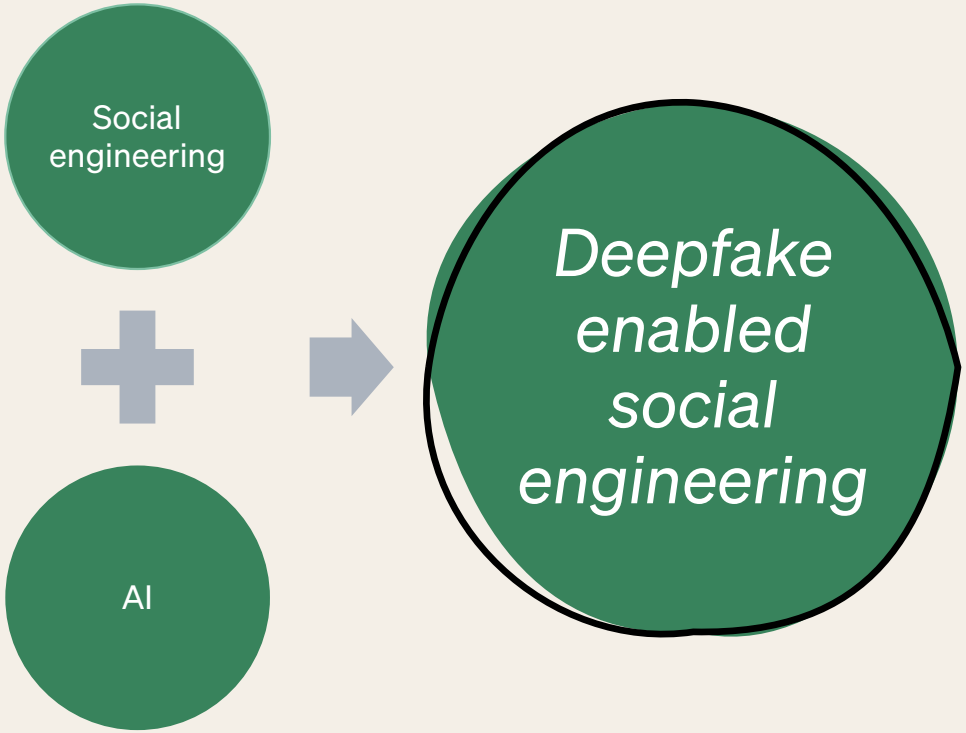
AI Acceleration Factor: Supply Chain Compromise



- AI maps vulnerabilities across global suppliers
- Automates exploit discovery at scale
- Increases speed of compromise and lateral movement

61% of US companies have experienced a software supply chain attack in the past year (Anchore, 2024)

AI Acceleration Factor: Social Engineering



- Voice & video clones impersonate leaders
- Used to authorize payments, share credentials
- “Trust factor” exploited in high-stakes scams

In 2024, a Hong Kong finance worker was tricked by a deepfake CFO call into wiring **$25M**

JPMorganChase

Deepfake Interactive Activity – Can you Spot the Deepfake?

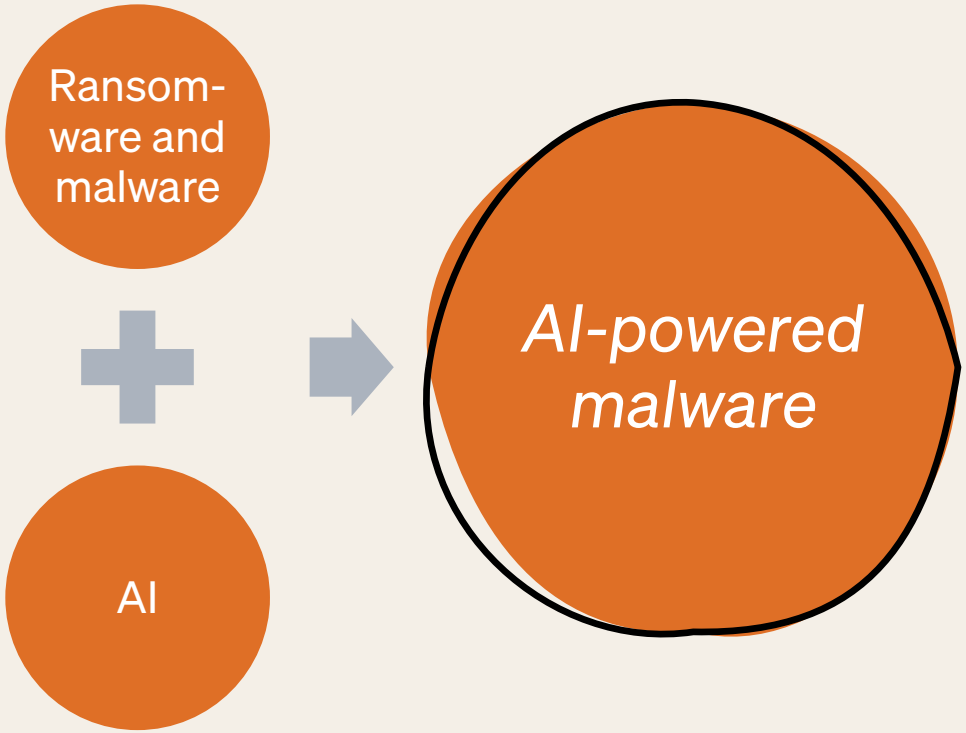
DIFFICULTY - MEDIUM

JPMorganChase

Deepfake Interactive Activity – Can you Spot the Deepfake?

DIFFICULTY - HARD

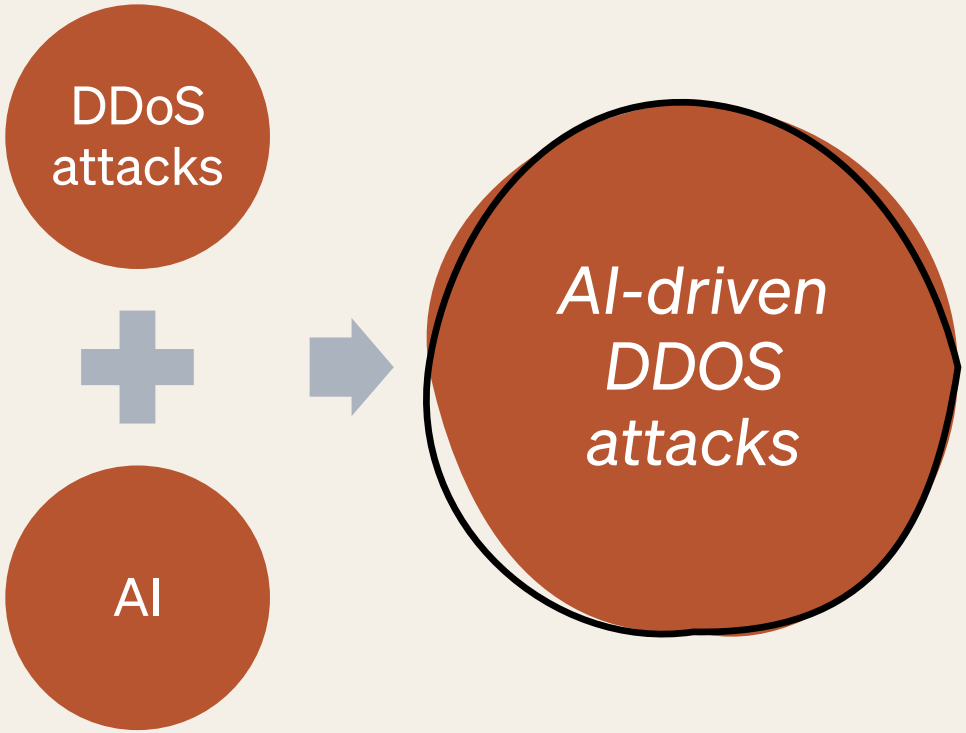
AI Acceleration Factor: Ransomware and Malware



- Generates polymorphic code that evades detection
- Learns and adapts to defenses in real time
- Malware-as-a-service now enhanced with AI

95% of malware strains observed in 2024 used polymorphic techniques (HP Wolf Security)

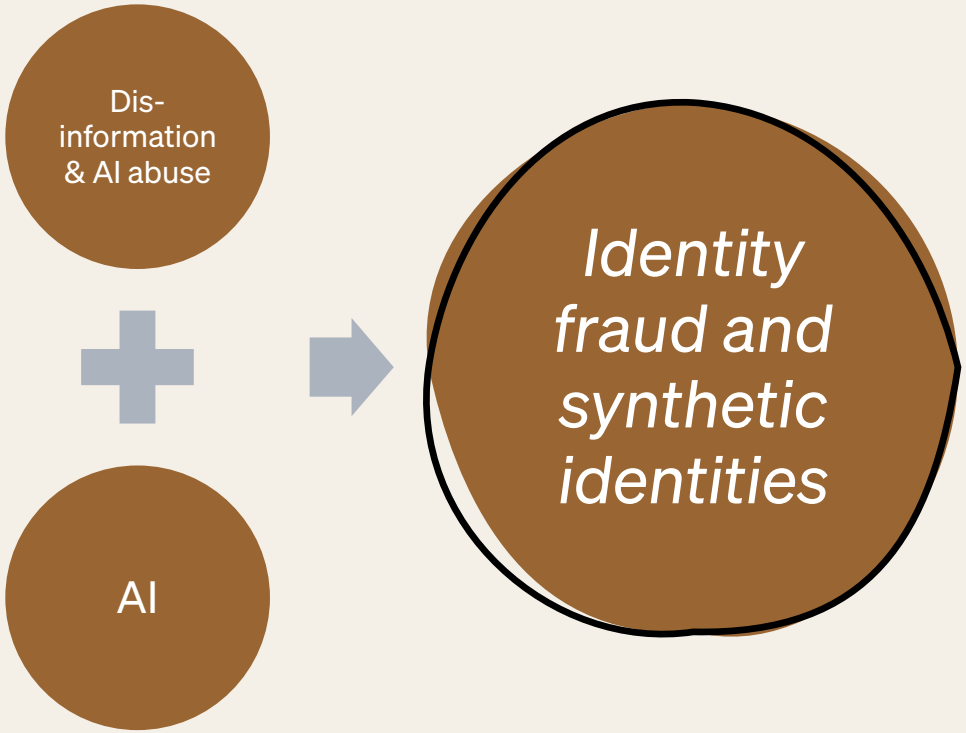
AI Acceleration Factor: Distributed Denial of Service



- AI optimizes botnet traffic for max disruption
- Targets shift dynamically to evade defenses
- Attacks scale faster than human response

In 2023, Google mitigated the largest DDoS ever at **398 million rps**—researched warned AI will drive the next surge

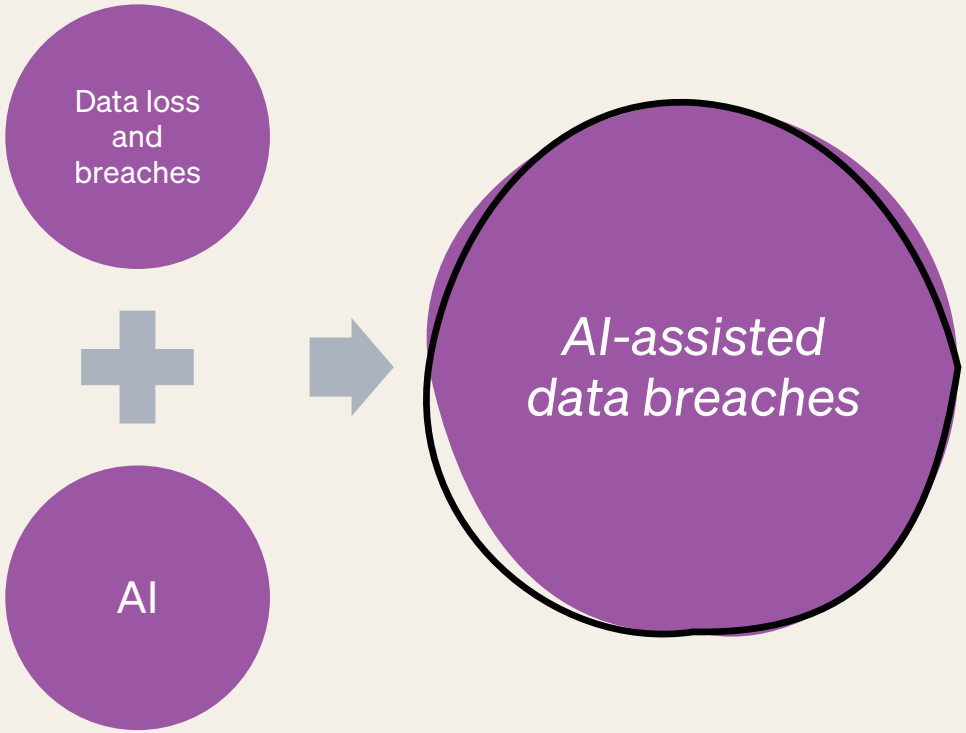
AI Acceleration Factor: Disinformation and AI Abuse



- AI creates realistic fake identities at scale
- Synthetic profiles pass KYC and onboarding checks
- Exploited for fraud, money laundering, and access

Synthetic identity fraud is the **fastest-growing financial crime**, costing US banks $20B+ annually (Aite-Novarica)

AI Acceleration Factor: Data Loss and Breaches



- AI accelerates data discovery & exfiltration
- Can quickly analyze stolen data for sensitive content
- Increases impact and resale value on dark web

The average global breach cost **hit $4.88M in 2024**, with AI-assisted data mining cited as an emerging driver (IBM)

Fraud & Attack Prevention

Critical Controls

- Enforce multi-factor authentication (MFA) everywhere possible
- Require dual authorization for high-value or international wires
- Implement velocity checks & anomaly detection (flag unusual payment patterns)

Response & Preparedness

- Maintain an escalation playbook for BEC, ransomware, and fraud alerts
- Run fraud drills with treasury and AP staff, simulating “urgent CEO wire” scenarios
- Pre-arrange contacts at bank fraud teams and law enforcement for rapid response

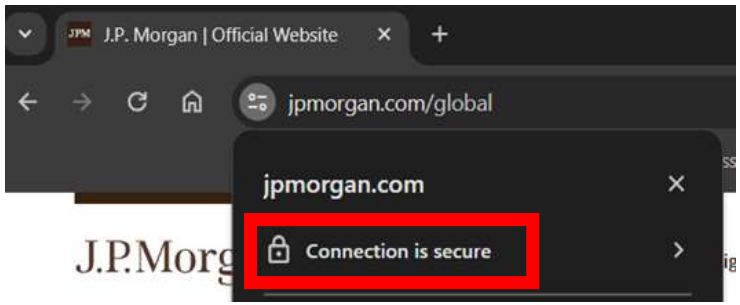
Additional Safeguards

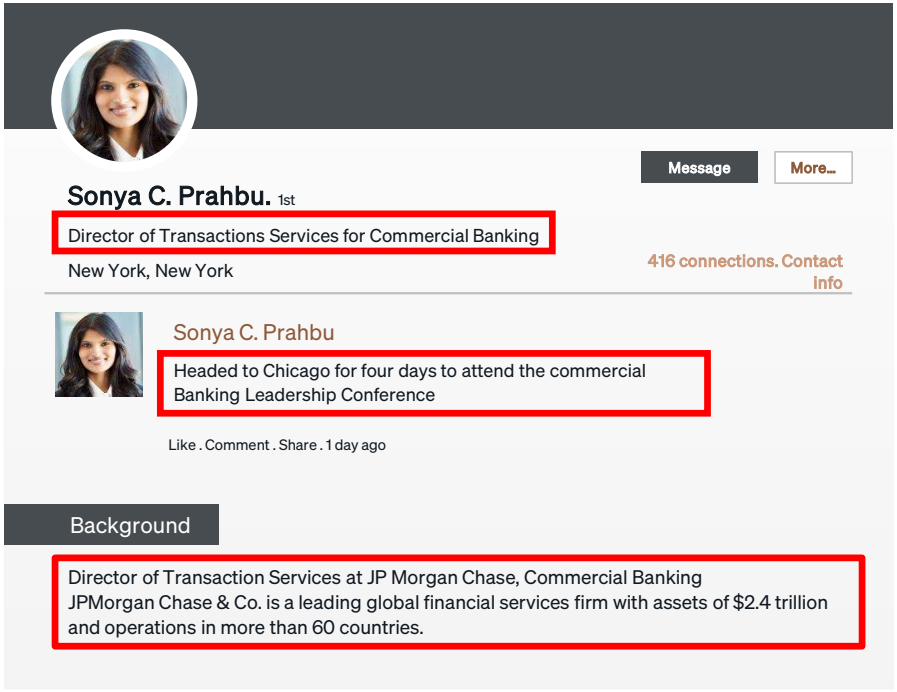
- Monitor for lookalike domains and spoofed vendor invoices
- Verify vendor and client account changes out-of-band (not by email alone)
- Integrate AI-driven tools to detect synthetic identities and fraudulent account openings

Protect Yourself

Online

- Activate Multi-factor Authentication (MFA) everywhere
- Always review the URL before entering credentials (password managers are good at this)
- Do not send personal and financials information via email
- Verify requests to engage with a company using contact info from a known source
- Look for the padlock on websites





Social Media

- Avoid the dangers of over sharing on social media
- Leverage policies and procedures that restrict employees from divulging personal information that can be used by cybercriminals

Business Continuity Planning (BCP) For AI-Driven Resilience

Driving thought leadership through Business Disaster Recovery Planning

- Provide best practices and guidelines to identify opportunities to improve your technology BCP against AI-accelerated threats
- Offer insights to assist with your AI-aware safeguards in your technology roadmap
- Based on best practices, help you develop a playbook to review system entitlements and detect anomalous access patterns
- Create and rollout strategy to ensure electronic payment and collection services operate securely, which can operate even if mail or physical facilities are disrupted
- Propose thought leadership and scorecards to measure resilience across treasury, payments and critical systems under various threat scenarios

1

Pre-Crisis

It is important to establish an AI-aware BCP pre-crisis to ensure essential services remain functional in the face of accelerated, automated attacks.

2

During Crisis

Deploy and tech systems and technology periodically with AI-enabled attack simulations to validate the applicability and performance of your plan.

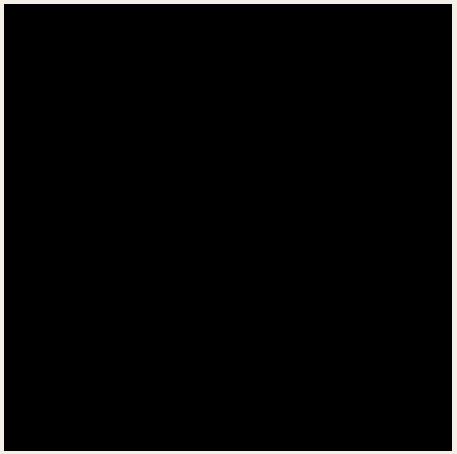
3

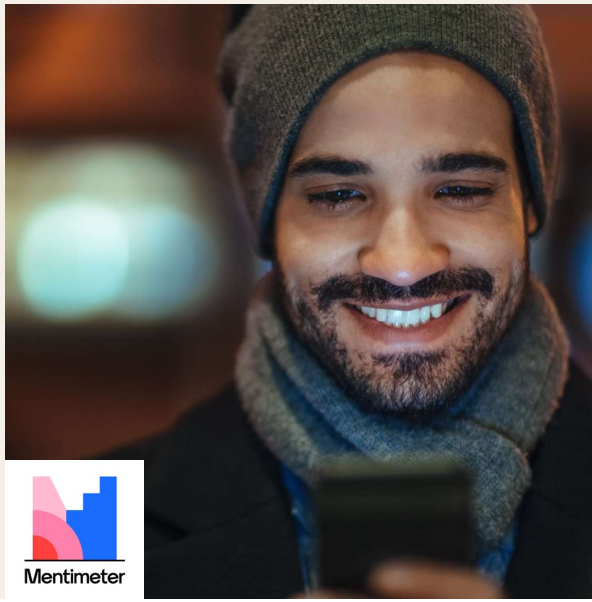
Post-Crisis

Conduct a review post crisis to incorporate lessons learned from incidents and employee feedback to improve the plan for the next event.

Test your knowledge – checkpoint #2

Ready to test your cyber knowledge?
Scan the QR code below or go to
menti.com and use code: 1363 8053





Identification and Restoration of Critical Business Processes is Essential

Identify Critical Business Processes

1

- What services are essential to achieving organizational goals?
- What services are you required to perform, by law, contract, even during cyber disruption?

Determine the Impact of a Disruption

2

- How long can the processes be down?
- Would the loss of the service cause reputational, financial, or regulatory harm in a breach scenario?

Prioritize Critical Business Processes and Functions

3

- What processes are truly mission critical?
- What payments must be protected first (e.g. critical vendors/suppliers, payroll, etc.)?

Identify Dependencies

4

- What technologies are my critical processes dependent upon (EDR, AD, cloud platforms) could AI-powered attacks exploit?
- To what vendor(s) have we outsourced critical processes?

Develop Contingency Plans

5

- Is there an alternate process to continue operations if disruption occurs?
- Do DR/BC plans account for AI enabled fraud, ransomware, or model poisoning? Have we tested those plans?

“Top 10 List” Of Effective Programs/Practices

Conduct an independent assessment

Continuous monitoring with AI-enabled detection

Deploy mandatory employee training and testing

Engage government and law enforcement

Simulate an internal attack

Third-party/vendor risk reviews with AI focus

Crisis-tested BEC & ransomware playbooks

MFA + layered payment controls

Understand how money leaves your organization

Cyber insurance aligned to new AI-driven risks

Payment Security & Controls

User Access

- Know who has access to your banking relationships and accounts; review entitlements regularly
- Set payment limits at account and employee level based on trends/history
- Establish multiple approval levels based on various thresholds
- Do not permit multiple users to log in from the same computer to initiate or release payments
- Use approved templates/verified bank lines and restrict use of free form payments
- Require multifactor authentication

Verification

- Don't move money based solely on email, text or phone instructions
- Perform callbacks for request for payments, changing payment instructions or contact information
- Conduct callbacks with the person making the request via a phone number from a system of record
- Don't used numbers obtained from sources like email, pop-up messages, texts or voicemail
- Never give information to an unexpected or unknown caller
- Establish with customers / partners how changes in account information will be communicated and validated
- Have a process to respond to your financial institution if they call about unusual payments

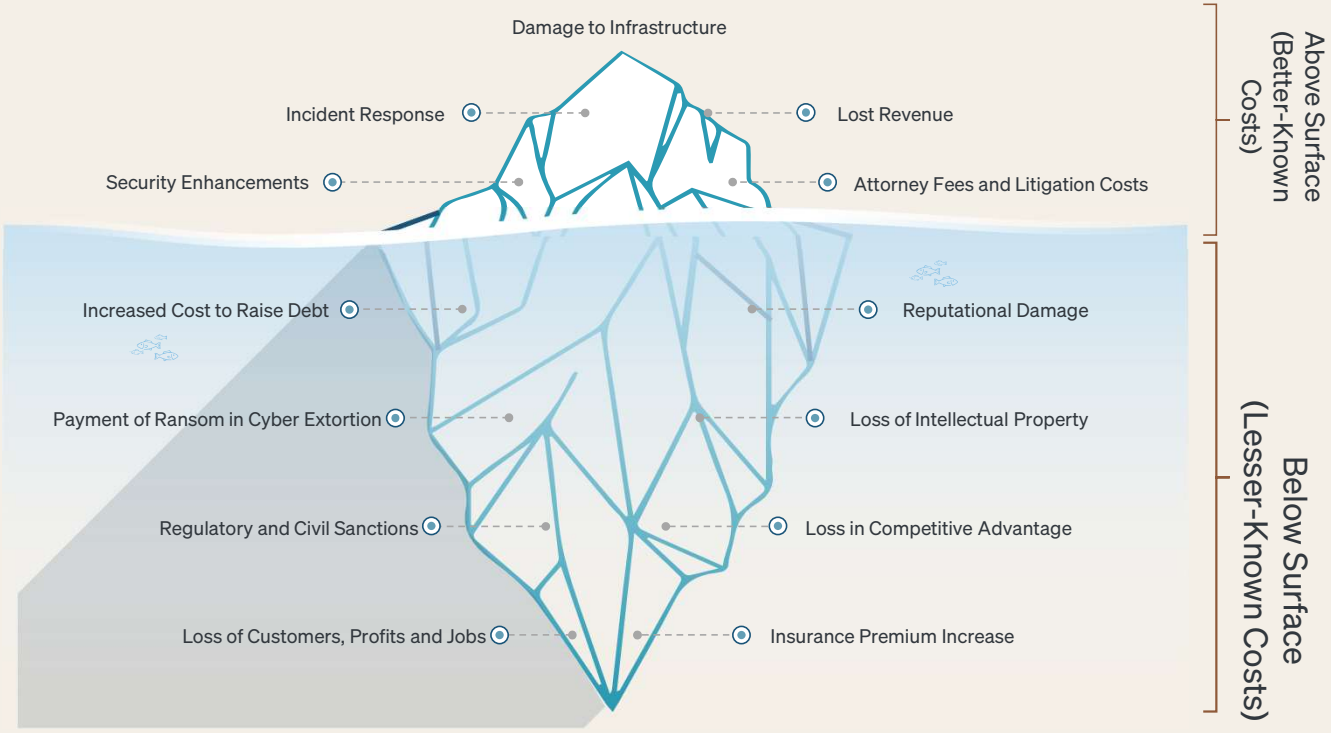
Reconciliation

- Perform daily reconciliation
- Validate that vendors have received payments on payment date.
- If volume is an issue, perform sampling or set thresholds such as validating payments over a certain amount

Insuring for The Worst-case Scenario

Cyber insurance is designed to help an organization mitigate risk exposure, through risk transference, by offsetting costs involved with recovery after a cyber-related security breach.

Costs of a Cyber Attack & Which Risks Insurance Can Transfer



Closing

AI is rewriting the threat landscape. *But resiliency is within reach.*

Awareness of the Threat Landscape	Take a proactive approach to identifying threats and assigning the appropriate risk and priority levels Understand the tactics, techniques and procedures employed by adversaries to defend against them effectively
Implementing new Technologies	Invest in new technologies such as post-quantum cryptography, AI/ML, next-generation firewalls, and more, to vouchsafe organizational security into the future
Employee Training and Education	Foster and promote a culture of reporting and awareness; training and testing regularly
Incident Response	Clearly define roles, responsibilities, and procedures to ensure timely response and recovery while minimizing incident impact and maintaining operational capabilities
Collaboration with Industry Partners	Share intelligence and collaborating on solutions for mutual benefit and preparedness across the industry
Continuous Assessment and Improvement	Stress test security controls and response plans on a regular basis to match the dynamic threat landscape

Disaster recovery in the AI era isn't optional—it's your competitive advantage.

Q&A | Discussion


JPMorganChase