J.P.Morgan

Modern Disaster Recovery & AI-Driven Threats

County Treasurers Association of Ohio | November 2025

Speaker Highlight

Sam Collis

Vice President, JPMorganChase

Sam Collis is a Cyber Resiliency Exercise Coordinator and Emerging Threats Analyst at JPMC, with 28 years of experience. He educates clients on cybersecurity and fraud prevention through presentations, workshops, and readiness exercises. His background includes roles in Accounting, Technology Operations, Risk & Controls, and Network Security.

Philip Soeder

Vice President, JPMorganChase

Phil Soeder is a Vice President at J.P. Morgan, specializing in client relationships and acquisition within the Government sector. He works closely with product specialists to deliver the firm's comprehensive suite of services to clients and prospects in Central and Northeastern Ohio and Pennsylvania. With over a decade of experience, Philip develops effective financial solutions tailored to his clients' unique needs and is recognized for his strong relationship-building skills.

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.

The New Reality of Cyber Threats

$10.5T — Expected cost of global cybercrime annually by 2025[1]

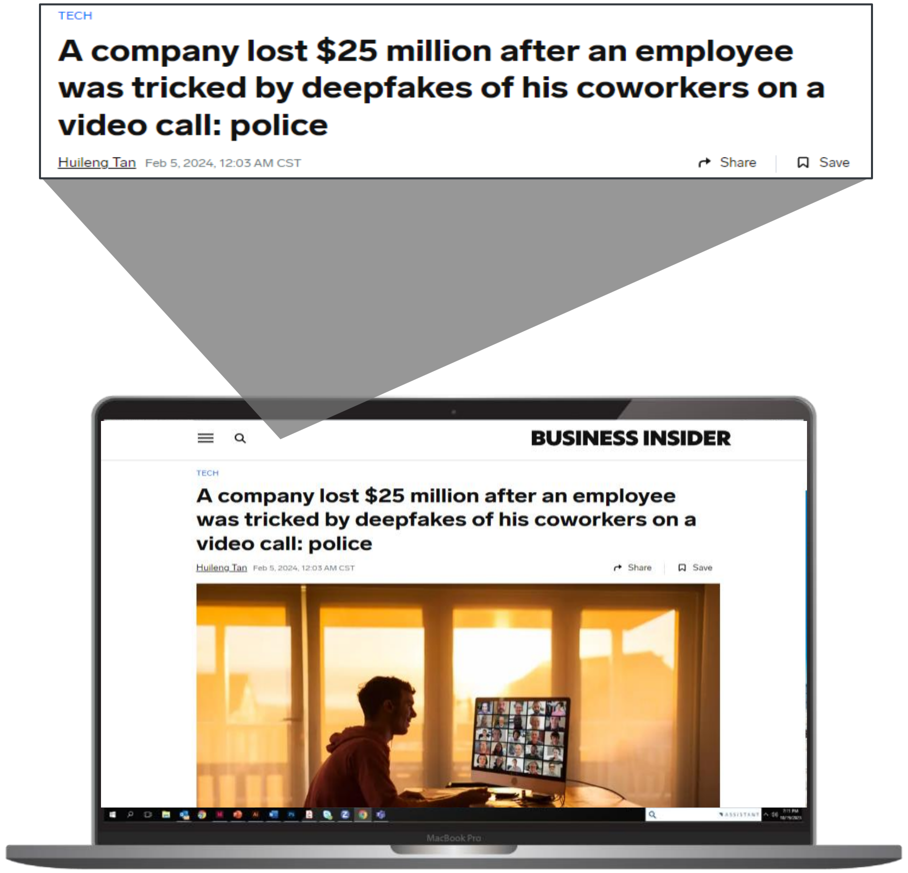
60% — Of participants fell victim to AI-generated phishing emails, a rate comparable to non-AI phishing crafted by experts[2]

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/

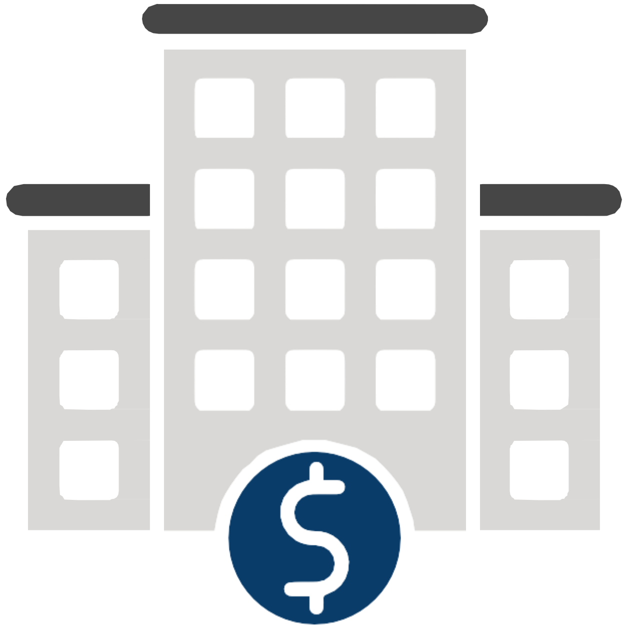
Bad actors continuously seek to leverage emerging technology and vulnerabilities to carry out malicious activity



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]



59%

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

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]

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

Threat Landscape: Addressing Today’s Top Cyber Trends

Continuous Improvement and Investment in our Capabilities

Supply Chain Compromise

Threat actors compromising an organization by targeting less secure partners of its supply chain. Rampant increase in Year over Year supply chain attacks.

Managing the Risk: Supplier Threat Intelligence, Third-Party Oversight, Asset Management, Vulnerability Management, Business Continuity Panning and identification of resilient alternatives (e.g., in house service)

Malware and Ransomware

Ransomware as a Service model enables cyber criminals to encrypt systems with ransomware and extort victims.
How we address the risk

Managing the risk: Antimalware, Data Backup and Recovery, Email and Web Content Filtering, Access Controls, Cyber Threat Intelligence, Security Monitoring, Digital Forensics

Social Engineering

Sophisticated Phishing, Smishing and Vishing campaigns are increasing with the use of AI. Vast majority of incidents start with social engineering.

Managing the risk: Security Awareness training, Email and web content filtering, Access Controls, Antimalware, Security Monitoring, Brand management services to prevent spoofing

Distributed Denial of Serivce (DDoS) & Internet Of Things (IOT) Attacks

DDoS attacks disrupt availability of services with flood of malicious Internet traffic. Compromise and abuse of insecure IOT devices to conduct DDoS attacks or gain access to networks.

Managing the risk: Inline DDoS protection, Cyber Threat Intelligence to monitor campaigns and targeting, Asset & Inventory Management, Network Access Controls

Disinformation and Artificial Intelligence (Ai) Abuse

Improper use of AI and synthetic media to deceive end users and perpetrate fraud. Increasing financial losses across payments and treasury departments.

Managing the risk: Awareness and fraud prevention training, collaboration with government and law enforcement, enhanced payment verification controls, investment in AI/emerging tech

Data Loss and Breaches

Loss of confidential information as a result of internal (e.g., human error or malicious insider) and external threats

Managing the risk: Data Loss Prevention, Blocking removable media, Information Classification and Handingling, Access Controls, and Data protections (e.g., encryption)

The Power of Artificial Intelligence

AI can empower organizations to drive growth in an increasingly competitive business landscape

Automated Processes

Data-Driven Insights

Personalization

Major Financial Impact

$4.4T Added to the global economy annually[1]

- Automation and Efficiency
- Data Analysis
- Customization
- Enhanced Security
- Analytics and Forecasting
- Innovation
- Process Optimization

CHALLENGES

- Data Quality
- Talent Gap
- Ethical Considerations
- Integrating Systems
- Trust
- Cybersecurity
- Cost and ROI

- Data Breaches
- Model Poisoning
- Bias and Discrimination
- Account Takeovers
- Synthetic Identity Fraud
- Insider Threats
- Deepfake Threats

[1] McKinsey & Company, *The economic potential of generative AI*, June 2023

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

Best practice

- Increase scrutiny around potential phishing emails and messages from other channels
- Continuously train and test employees
- Use multifactor authentication to prevent attackers from getting in using legitimate credentials

Deepfake

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

Best practice

- Limit audio and video exposure on publicly accessible platforms – even small snippets can be used to create a deepfake
- Do not rely solely on voice or video authentication
- Follow established procedures around payments and account changes

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.)

Best practice

- Use and verify trusted sources for information and news
- Update privacy settings on social media and other publicly visible accounts; use a VPN
- Limit the amount of personal content posted to social media

AI Present & Future: Limitations, Considerations, & Misconceptions

Overreliance and Value misalignment
- Decline of essential human skills over time
- Degradation of human intelligence and knowledge
- Value lock-in
- Skewed decision making

Doing AI the right way
- Continuous monitoring and transparency
- Explicit programming
- Regular audits and scrutiny

Data Errors
- Not all data is equal
- Data must be properly cleaned/filtered
- Models must fit the data
- The data must be balanced
- The model results must be interpreted properly – models can be too accurate

AI is neutral and unbiased

“Terminator” situation/sentient AI

AI, ML & DL are the same

AI will take away all jobs

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 a pre-crisis BCP to create a set of strategies and preventative action plans to ensure full functionality of essential services in a disaster recover scenario.

2

During Crisis

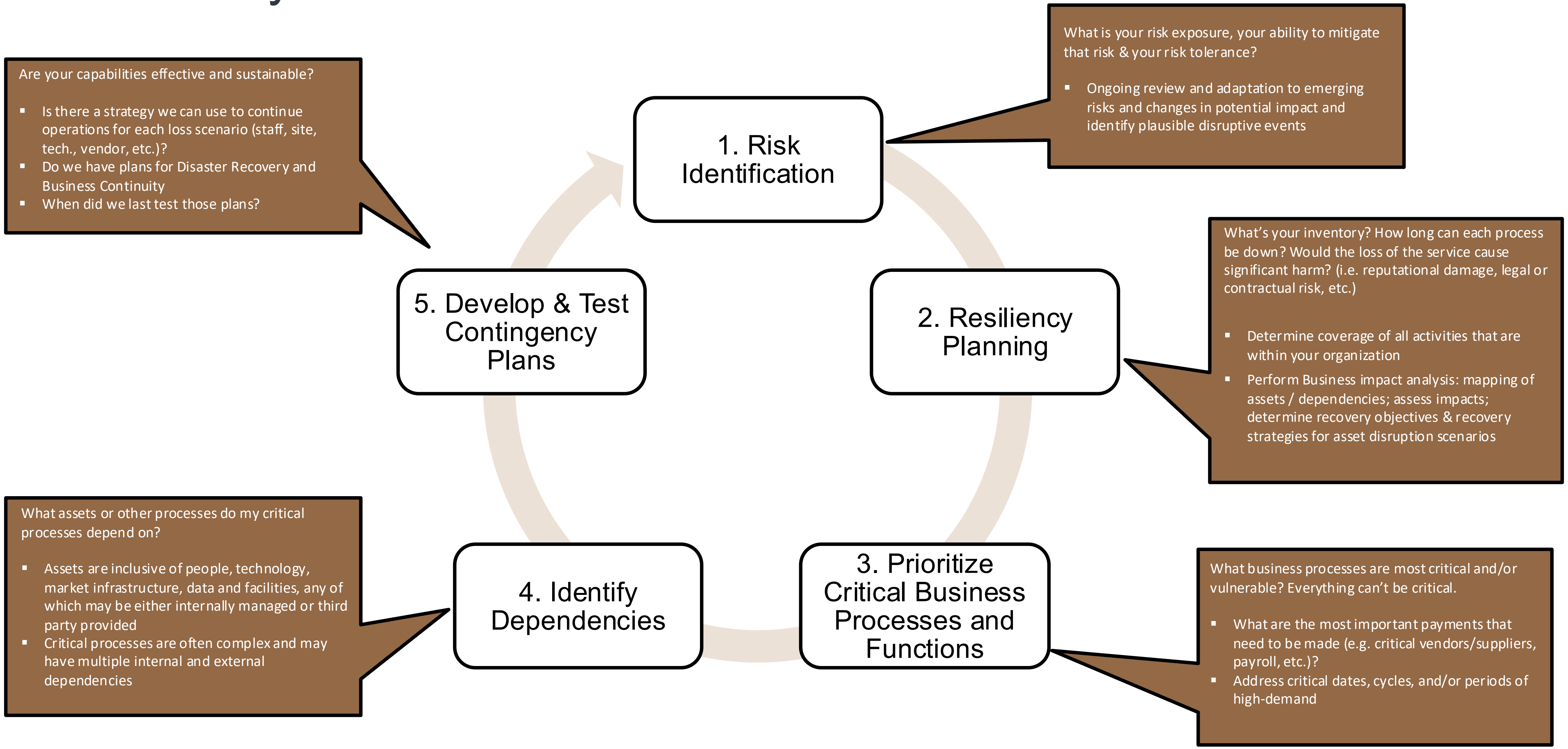
Deploy BCP, assess the situation and follow the pre-defined procedures to contain the incident and begin recovery operations.

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.

Business resiliency programs continuously identify and manage risk across a lifecycle



Resiliency is paramount in the face of today's evolving threats

Awareness of the Threat Landscape	Taking a proactive approach to identifying threats and assigning the appropriate risk and priority levels Understanding the tactics, techniques and procedures employed by adversaries to defend against them effectively
Implementing new Technologies	Investing 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	Fostering and promoting a culture of reporting and awareness; training and testing regularly
Incident Response	Clearly defining roles, responsibilities, and procedures to ensure timely response and recovery while minimizing incident impact and maintaining operational capabilities
Collaboration with Industry Partners	Sharing intelligence and collaborating on solutions for mutual benefit and preparedness across the industry
Continuous Assessment and Improvement	Stress testing security controls and response plans on a regular basis to match the dynamic threat landscape

Problems Faced by Treasurers and County Officials

VENDOR DESK

"I can't keep up with the relentless pace of vendor onboards and changes.

ACCOUNTS PAYABLE

"People are constantly bombarding me with requests to circumvent our procedure 'just *this once*'

PROCUREMENT

"We need to check the sanctions lists with every PO we issue.

FINANCE

"It's impossible to fully execute our payables strategy.

RISK

"We are about to lose our insurance coverage.

HOW AI CAN HELP

VENDOR DESK	ACCOUNTS PAYABLE	PROCUREMENT	FINANCE	RISK
Automate and organize manual tasks	**Standardize and strengthen the process to guard against the bad guys**	**Ongoing sanctions monitoring + internal compliance controls**	**Integrate the payables strategy execution into the vendor onboarding process**	**Trackable, auditable vendor management process = fraud liability waiver**

Potential AI use cases for Treasurers and County Officials

INSIGHTS

Cash Forecasting

Accelerate forecasting, boost analytics and decision-marking capabilities and deliver actionable insights

Payment Channel Optimization

AI powered platforms and tools to intelligently route payments to vendors

Fraud Detection

Identify fraudulent activities / new patterns / payment anomalies to reduce client's risk exposure

Supplier / Customer KYC

Account Validation, Entity Validation

INQUIRE

Developer Portal

Developers can ask questions instead of searching through developer documentation

Virtual Assistants

Respond to inquiries more naturally and handle more complex questions

Dispute Resolution

Summarize unstructured responses from merchants and customers during the dispute review process

Guides & Documents

Synthesize content from various guides (market practices, regulations, payments format, etc.) as well as onboarding docs

TRANSACT

Payment Initiation

Initiate payments with instruction / file generation and automated data input supported by AI

Payment Authentication

Apply AI tools for payment authentication / approvals with enhanced efficiency & controls

Document Generation

Help generate various client documents such as bank letters, audit confirmations; pre-fill account opening documents

Receivables Recon

Improve the linking of payments to their corresponding invoices

For discussion

Q & A | Discussion