

Cybersecurity & Fraud Protection Webinar

November 2024

Today's hosts



Joseph Scharf

Sr Treasury Management Officer –
Government Banking - JPMorgan



Charles Million

Sr Treasury Management Officer –
Government Banking - JPMorgan

Cybercrime in the headlines 2024

Critical Infrastructure

Chinese hackers target water treat plants, electrical grid and transportation systems ¹
Attacker: State-Backed Hackers

Everyday Attacks

In 2023 three in four companies were at risk of a material cyberattack: Forecast \$452 billion this year ²

State Sponsored

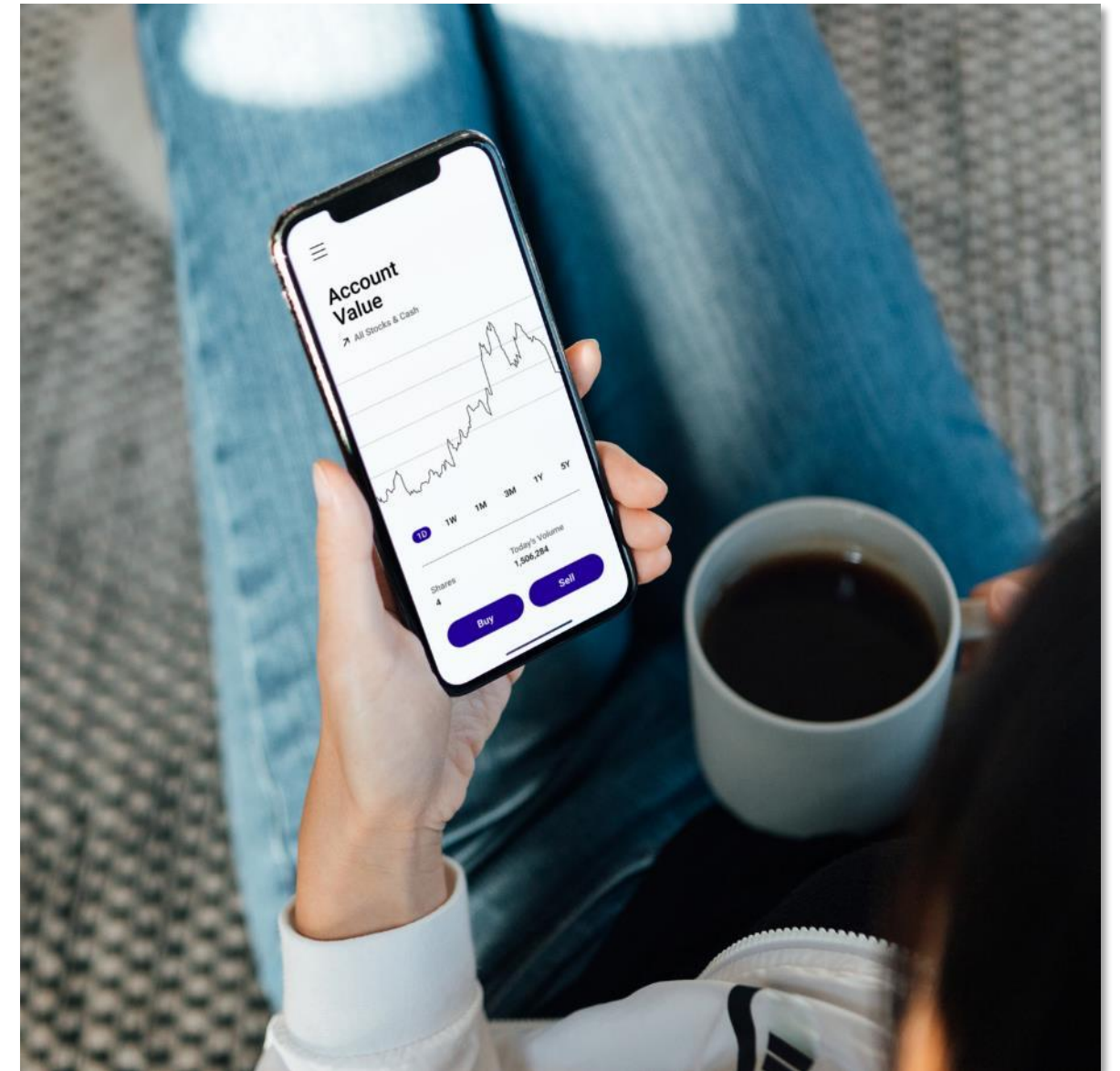
New Zealand, UK and Australia among countries targeted by state sponsored cyber espionage³
Attacker: Likely China

Preventable Attacks

Legacy test account breach provides gateway to senior leadership accounts⁴
Attacker: State-Backed Hackers

Deepfake

Attempt to deceive employee with deepfake audio impersonation of CEO⁵
Attacker: Unknown



¹ The Associated Press, [US says it disrupted a China cyber threat, but warns hackers could still wreak havoc for Americans](#), January 31, 2024

² Statista, [The impact of cybercrime on companies in the U.S.](#), February 5, 2024

³ Los Angeles Times, [New Zealand joins the U.S., U.K. in alleging it was targeted by China-backed cyber-espionage](#), March 26, 2024

⁴ The Associated Press, [Microsoft says state-backed Russian hackers accessed emails of senior leadership team members](#), February 2, 2024


⁵ CyberRisk Alliance, [LastPass thwarts attempt to deceive employee with deepfake audio](#), April 12, 2024

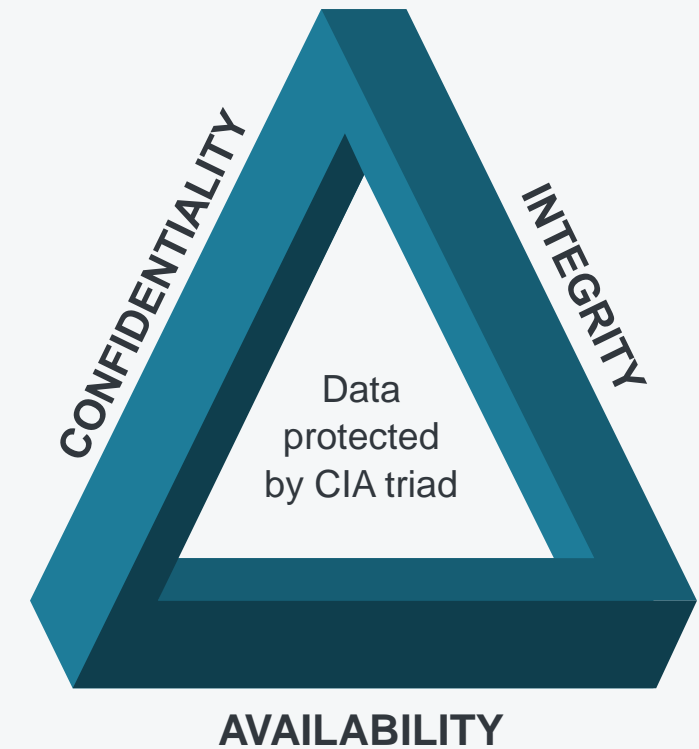
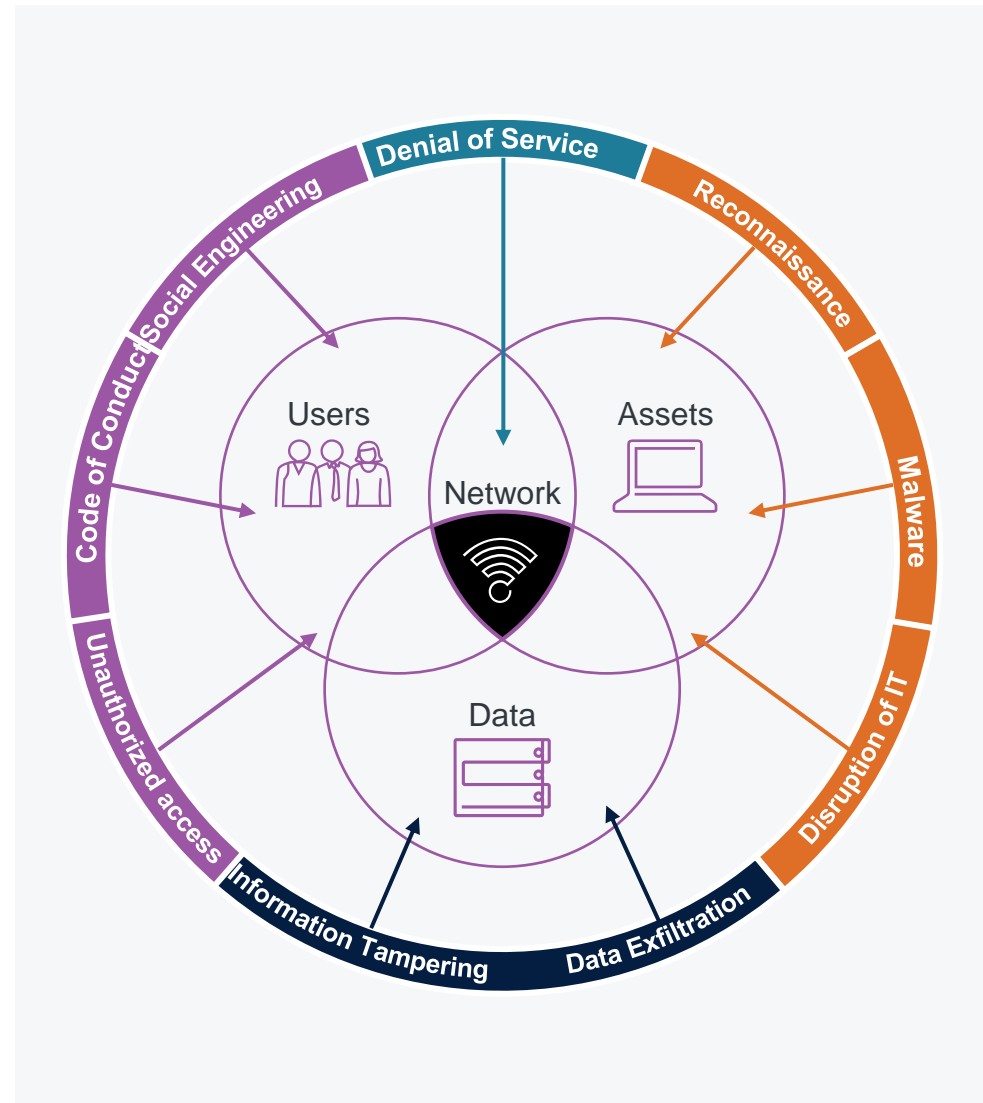
Primary targets & vectors of attack

In 2023, a cyberattack took place every

39 seconds¹ 

● Cybercriminals target key components that keep your business running. Consider your:














- Data
- Intellectual Property
- Software and OT Systems
- Money
- People 



¹ WatchGuard, [There was a cyberattack every 39 seconds in 2023](#), January 2024

Current and emerging threats

Every company, regardless of size or Industry, is at risk to common threats:

 	Business Email Compromise	 	Social Engineering
 	Fraud		Ransomware
	Systems Vulnerabilities		Outdated Software/ Hardware
 	Insider Threats	 	Human Error Ignorance



¹ 2023 FBI IC3 Report

Current and emerging threats

The attack surface is expanding...

 29.4B

IoT Devices Coming Online by 2030¹

Ransomware and Business Email Compromise continue to drive the bulk of attacks

Cloud attacks are increasingly successful, due to lagging maintenance and misconfiguration



Remote working presents risk, due to misconfigured cloud security measures / insecure home devices

Multifactor Authentication is becoming less secure, due to phone and SMS hacks

Outdate systems

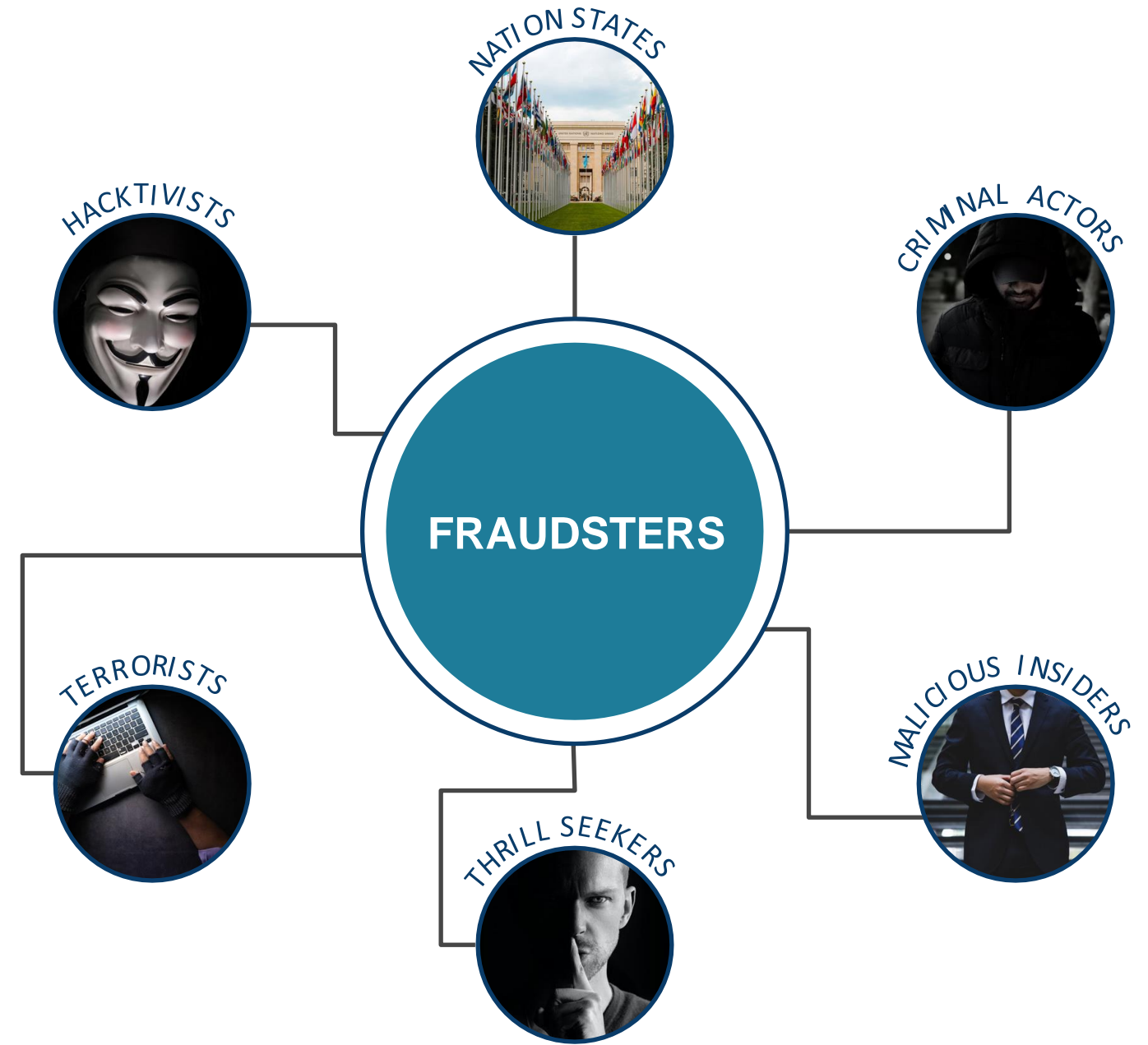
Attacks have shifted to 5th Generation

Attacks on the rise: Operational technology, quantum computing, AI, and IoT

1. Statista: [Number of IoT connected devices worldwide 2019-2023, with forecasts to 2030](#)

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 for perceived slights
- 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



How “they” do it

Hiding in Plain Sight – Social Engineering

- Job postings and interviews, free lance platforms
- Account take over, hijacking
- Identity theft, new account stolen identity
- Poisoned files like PDFs (resumes, job applications, etc...)
- Business email compromise
- Phishing/SMSishing/Vishing
- Residential proxies, caller ID
- System vulnerabilities, outdated software
- Insider threat
- Human ignorance



2:07

Fastest recorded eCrime¹

¹ CrowdStrike 2024 Global Threat Report

Why it matters

Cybercrime impacts national security

- Hostile nations acquire/laundry illicit profits fueling weapons programs, more sophisticated attacks and cyber warfare
- Multiple simultaneous critical infrastructure attacks
- Supply chain, essential service disruption
- Defense systems and government network intrusion, theft of secrets
- Political and ideological manipulation



You will have about **62 minutes** to secure the intrusion and minimize damage¹

¹ CrowdStrike 2024 Global Threat Report

Our commitment

At JPMorgan Chase, we invest in a robust Cybersecurity Program—with a risk management framework to identify, measure and address different cyberthreats.

Our top priority is to protect our clients and partners by sharing insights that help **you prevent, detect and respond.**

\$17B

Invested in Technology Annually

60,000+

Global Technology Workforce

2,000+

Artificial Intelligence / Machine Learning Experts

24/7

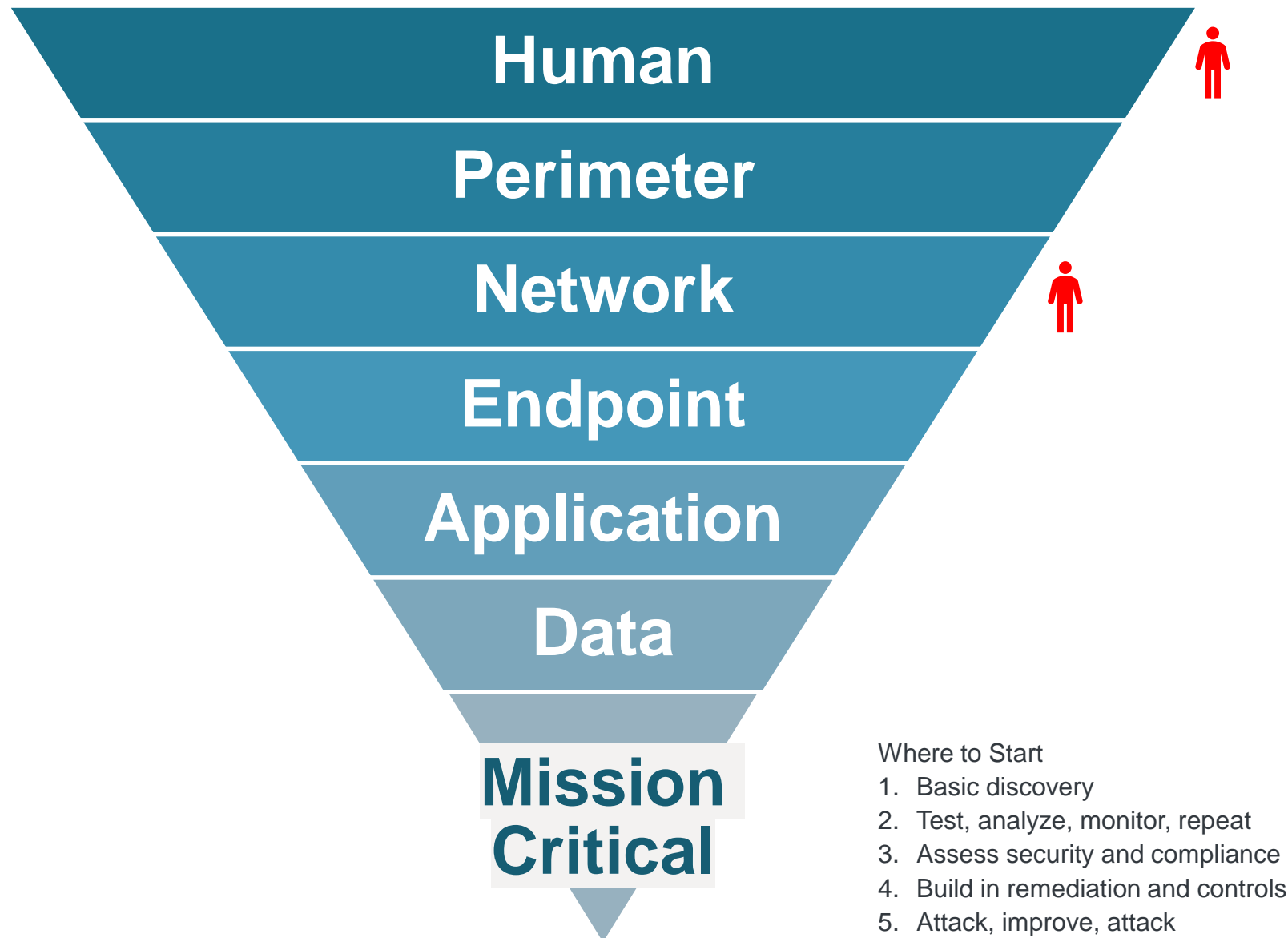
Follow-the-Sun Operation Model

3,100+

Cyber Investigations Per Year

Defense in-depth

Companies should build and leverage technology to detect fraudulent activity and attacks across high and low value asset types.



Layer 7 (Human):

Phishing tests, social engineering training, access management controls

Layer 6 (Perimeter):

Physical security, industry intelligence, malware, endpoint security & brand protection

Layer 5 (Network):

Unauthorized access, zero trust, API configuration

Layer 4 (Endpoint):

Protect network and additional unauthorized access

Layer 3 (Application):

Protect applications, Software Development Life Cycle (SDLC) and internal app security

Layer 2 (Data):

Security controls, in transit and at rest

Layer 1 (Mission Critical):

The organizations most critical data

The Power of Artificial Intelligence

AI can empower business 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 annually¹

Opportunities

- 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


Cyber & Fraud Threats

- 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

Deepfakes | The dark side of Artificial Intelligence

Improper use of AI and synthetic media pose a threat to national security, law enforcement and the financial domain

 **Deepfakes** are realistic, AI-generated videos, images, audio, and text of events designed to deceive targeted groups or individuals

- Inclination to believe what you see makes them effective in spreading mis/disinformation
- Low cost of resources needed to produce them raises the likelihood of successful attacks

 **In practice**, threat actors leverage chatbots and technology developed from large language models to simulate human activity

- Business Email Compromise
- Spear-phishing
- Fake websites and profiles
- Ransomware
- Voice clones for imposter scams, extortion and financial fraud

Example Deepfake Online



Multi-faceted mitigation is critical

- Collaboration between cyber professionals, financial institutions and law enforcement
- Public education, awareness and media literacy
- Regulation
- Detection mechanisms via AI/ML innovation (real-time monitoring, anomaly detection and incident response protocols)

Ransomware

Ransomware Payments Exceed Over \$1 Billion

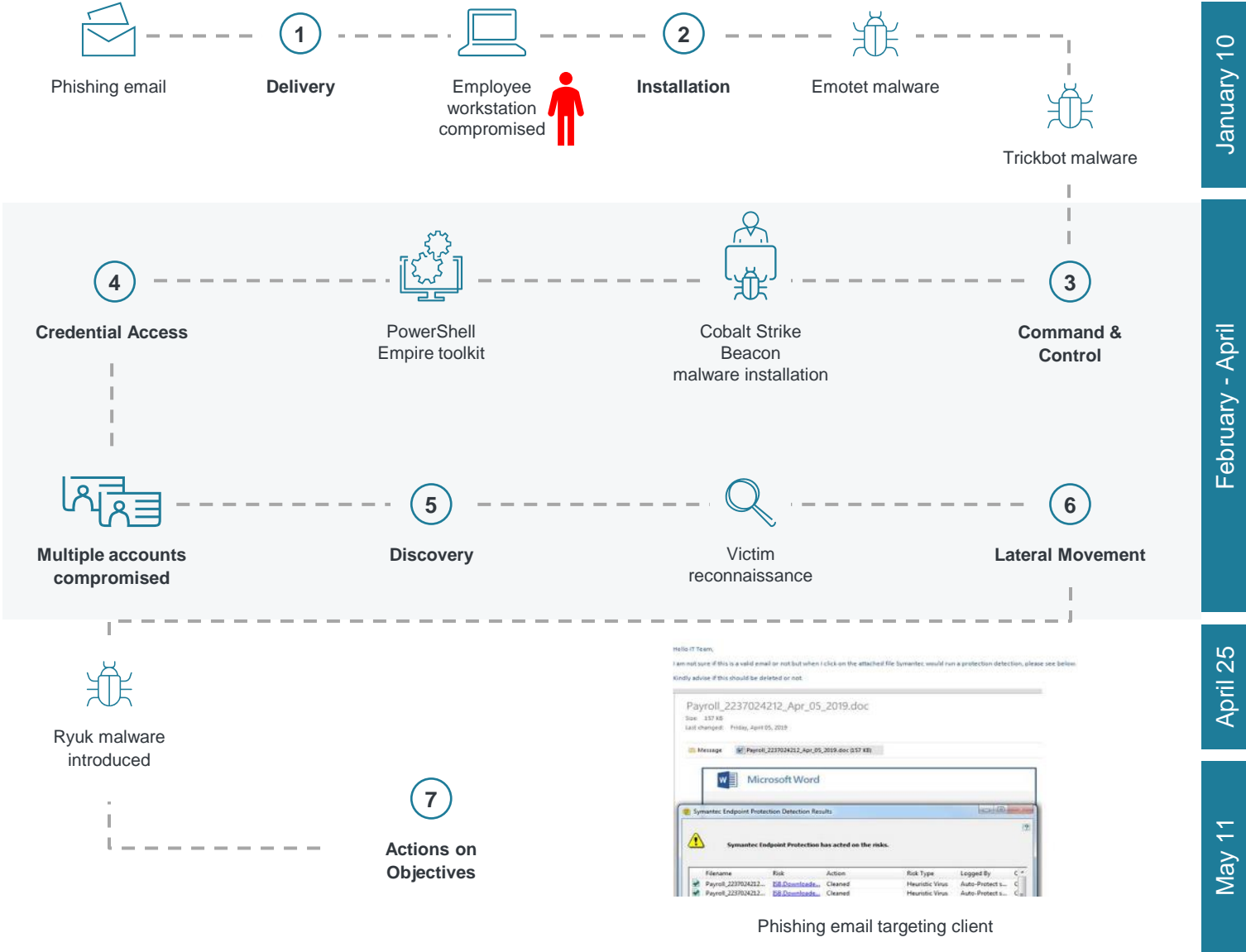
In extorted cryptocurrency payments from victims in 2023¹

- Loss of the ability to run your organization and potential permanent loss of data
- Key considerations:
- How much is the ransom?
- Should I pay ransom?
 - The FBI does not support paying a ransom to a cybercriminal.
 - Payment does not guarantee an organization will regain access to its data.
 - Paying the ransom may embolden cybercriminals to launch more attacks.
 - How do I ensure my company is resilient?



¹ Chainalysis, [Ransomware Payments Exceed \\$1 Billion in 2023, Hitting Record High After 2022 Decline](#), February 7, 2024

Anatomy of a ransomware attack



Business email compromise (BEC) & impersonation



- Cybercriminals use executive, business partner and vendor email impersonation to trick you into sending them money or data. Common tactics include:
 - Phishing attacks
 - Use of compromised email accounts
 - Claims a bank account can't be used due to an audit
 - Multiple account changes sent to victim during attack
 - Use of inbox email forwarding rules to send emails to fraudsters

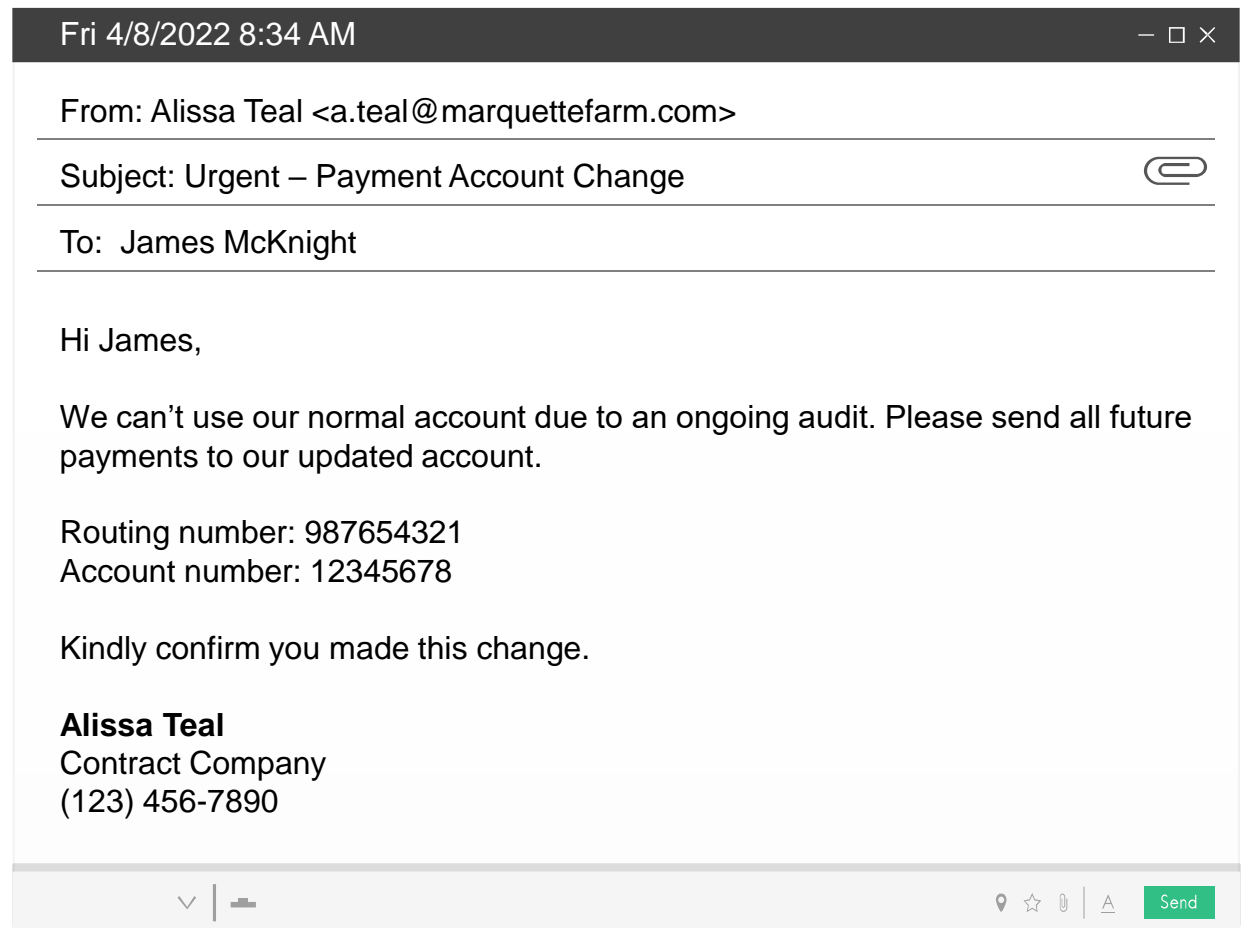
21,489 | Victims reported to the FBI¹

\$2.9B | Losses reported to the FBI¹

Criminals Register Look-alike Domains

Good domain:
marquettefarm.com

Bad domains:
marquettefarm**s**.com,
marquette**fram**.com,
marquettefarm.**co**,
mar**g**uettefarm.com,
marqu**ete**farm.com



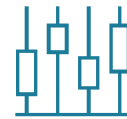
² 2023 FBI IC3 Report

BEC prevention & response



The Critical Control

- ✓ Perform a callback to the person making the request
- ✓ Use a phone number retrieved from a system of record to validate requests for payment, change of payment instructions or contact information
- ✓ Reject out of band payment processes



Additional Controls

- ✓ Establish written policies implementing mandatory callbacks
- ✓ Take calls from your bank regarding unusual transactions seriously
- ✓ Train employees on internal payment verification policies and BEC threats
- ✓ Encourage employee questions and holding a payment if it's suspicious



Response

- ✓ Notify your bank immediately
- ✓ File a report with the FBI's Internet Crime Complaint Center
- ✓ Contact your local FBI field Office
- ✓ Notify other law enforcement agencies as appropriate

These steps are critical to maximize chances for recovery

Check fraud is on the rise

Whether theft, forging or counterfeiting, check fraud continues to be a problem—and your organization needs to plan for it.

 **63%**

of organizations reported being impacted by check fraud¹

 **\$21 B**

check fraud losses in the Americas represented nearly 80% of global total²

Front-Of-Check Fraud

Altered Checks | Criminals alter the name or payment amount before depositing

Counterfeit Checks | Criminals use printers and desktop publishing software to create counterfeit checks

Back-Of-Check Fraud

Improper Endorsements | Criminal forges endorsement, or chooses not to endorse at all

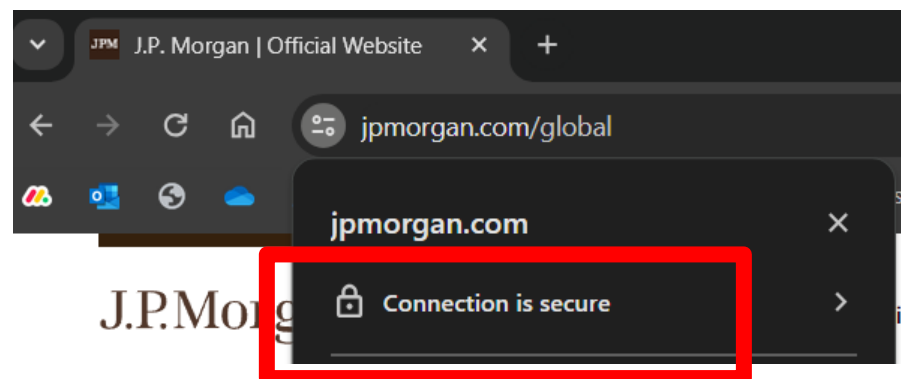
Mobile Deposit Fraud | Usually perpetrated by the intended recipient, sometimes to double-cash paychecks

¹ 2023 Association for Financial Professionals (AFP) Payments Fraud Survey

² Nasdaq, 2024 Global Financial Crime Report

Protect yourself

- 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
- Activate Multi-factor Authentication EVERYWHERE!
- Always review the URL before entering credentials (password managers are good at this).
- Be suspicious of unexpected phone calls
- 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



A LinkedIn profile page for Sonya C. Prahbu. The profile includes a circular profile picture, a 'Message' button, and a 'More...' button. The text below the profile picture reads: 'Sonya C. Prahbu · 1st', 'Director of Transactions Services for Commercial Banking', and 'New York, New York'. To the right of this text is '416 connections · Contact info'. Below the profile picture is a post by Sonya C. Prahbu: 'Headed to Chicago for your days to attend the commercial Banking Leadership Conference. I'll be leading a discussion on the future of transaction services and technologies'. Below the post are the options 'Like · Comment · Share · 1 day ago'. At the bottom of the profile is a 'Background' section with the text: 'Director of Transaction Services at JP Morgan Chase, Commercial Banking JPMorgan Chase & Co. is a leading global financial services firm with assets of \$2.4 trillion and operations in more than 60 countries. I lead a great team of 30 Technologists, located around the world. Together we determine and drive the technology solutions for all JP Morgan Chase's Commercial Banking transactions – managing millions and millions of dollars every hour !'. The text in the 'Background' section is highlighted with a red box.

Assessing and planning

Prioritize Your Risk, Assets and Threats

- Time is money and cybersecurity is a critical business decision
- Be proactive and vigilant now, to protect your organization's data, finances and business processes. Fortify your defense strategy.
- Define and enforce a cybersecurity policy
 - Key considerations: data loss prevention standards, software updates, social media requirements, encryption and content sharing, employee training, network access, incident reporting process

Measure and Plan

- Set goals and KPIs (*e.g., days to patch, meantime to detect and respond, employee training effectiveness*)
- Create a playbook
- Remain vigilant

Cyber Budgeting

- Optimize for ROI (*e.g., overlapping solutions, update software/hardware*)
- How to Budget (*e.g., best vs. effective/right size, understand actual vs. perceived threats, reduce attack surface*)



\$4.45M | Average Cost of a Data Breach Globally¹

\$9.48M | Average Cost of a Data Breach in the US¹

¹IBM Security: Cost of a Data Breach Report 2023

Set goals & KPIs

- Days to patch
- Meantime to detect, respond & recover
- Supply chain safety ratings
- Tabletop simulations
- Employee training effectiveness



Create a playbook & remain vigilant

A risk management plan is critical to help your company reduce exposure to cyberthreats.

Include steps to protect, identify, detect, respond and recover from an attack. Continually update, refine and test your defense strategies to combat risks. Identify:

- ✓ Stakeholders
- ✓ Critical Systems
- ✓ Required Actions and Recovery Processes
- ✓ Ways to Make Your Plan Evergreen
 - Consider Tabletops, Trainings and IT Skill Development

[National Security Agency Top Ten Cybersecurity Mitigation Strategies](#)

Q&A | Discussion

Use the **Raise Your Hand** feature to ask a question.



Appendix

- [❑ Cybersecurity and fraud protection insights](#)
- [❑ Phishing](#)
- [❑ Phishing indicators](#)
- [❑ Payment security & controls](#)
- [❑ Who are “they” \(nation state threat actors\)](#)
- [❑ Counter measures to Nation State cyber attacks](#)
- [❑ Ransomware chain of custody](#)
- [❑ Quantum computing](#)
- [❑ What to expect when check fraud happens](#)
- [❑ Prioritize your risk, assets and threats](#)
- [❑ Cyber budget](#)
- [❑ Cyber budget optimization](#)
- [❑ Define and enforce a cybersecurity policy](#)
- [❑ Insuring for the worst-case scenario](#)

Cybersecurity and fraud protection insights

- Contact your J.P. Morgan Chase relationship team with questions.
 - Visit [Commercial Banking Insights](#) and [Fraud Solutions](#) for resources to mitigate threats.
 - Visit www.ic3.gov for updated PSAs regarding BEC trends and other fraud schemes.
-
- For immediate assistance regarding electronic fraud matters after 5 p.m. EST
 - **J.P. Morgan Access®**: 866-872-3321
 - **Chase Connect®**: 866-619-3053, Option 1

The screenshot displays the J.P. Morgan Chase Commercial Banking website. The navigation bar includes links for Solutions, Industries, Insights, Client Stories, Impact, Contact Us, and Login. The main heading is "Cybersecurity and Fraud Protection". Below this, there are six featured articles, each with a representative image and a title:

- Report: Most companies will experience fraud >** (Image: A person sitting on a ledge by a window, working on a laptop.)
- How smaller companies can fight fraud with limited resources >** (Image: A person working at a desk in a modern office environment.)
- Protect your organization against ransomware >** (Image: A group of people in a meeting room, with one person in a wheelchair.)
- Does your disaster recovery plan cover ransomware attacks? >** (Image: Close-up of hands typing on a laptop keyboard.)
- 12 tips for mitigating cyberattacks >** (Image: A long aisle in a server room with rows of server racks.)
- Developing a proactive mindset on ransomware >** (Image: A close-up of a server rack with glowing lights.)

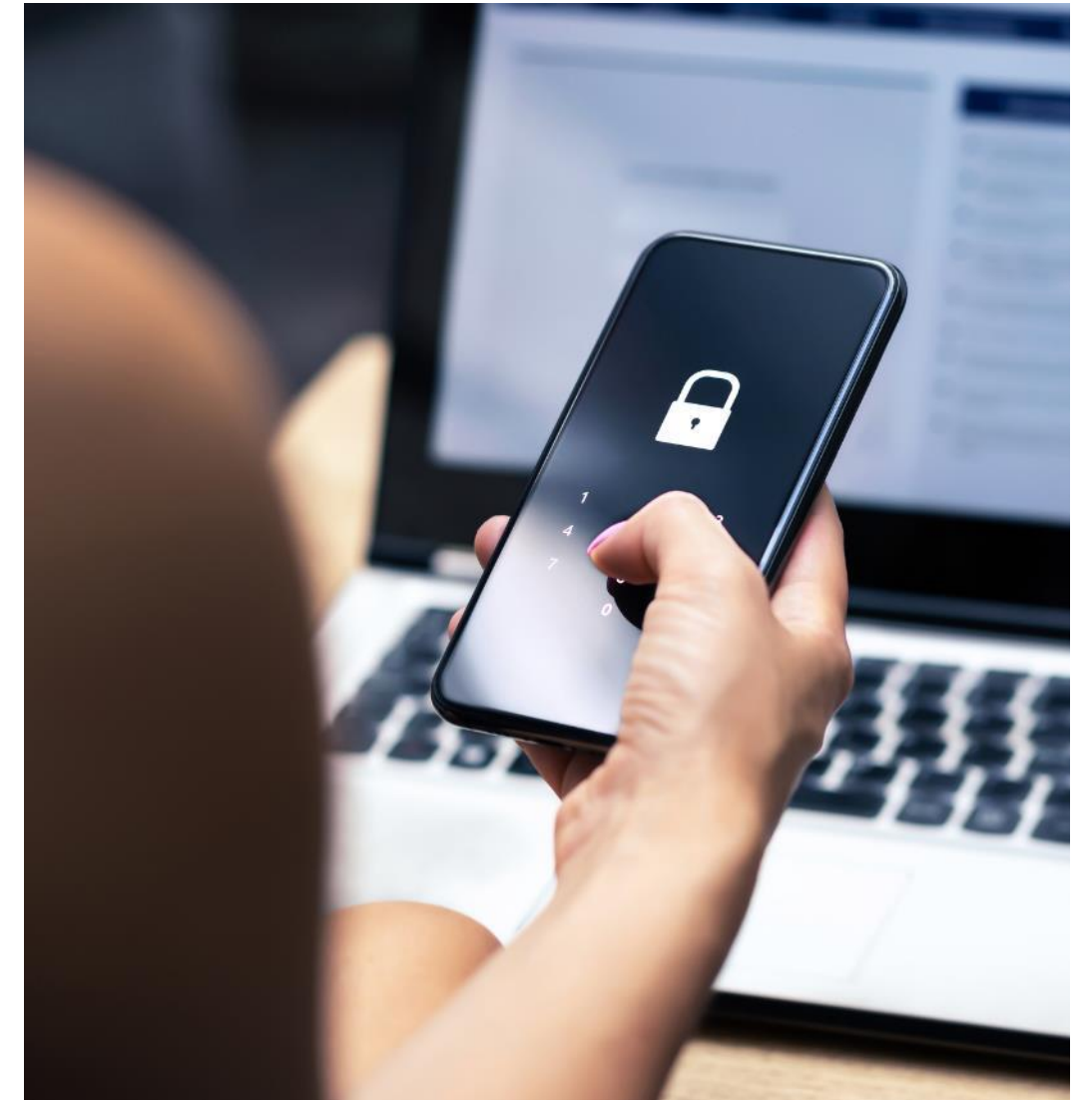
Phishing

 **298,878**

Victims reported to FBI in 2023¹

Practice of sending blanket emails to large groups or targeted emails to individuals as means to commit financial fraud or infect or gain access to systems.

¹ 2023 FBI IC3 Report



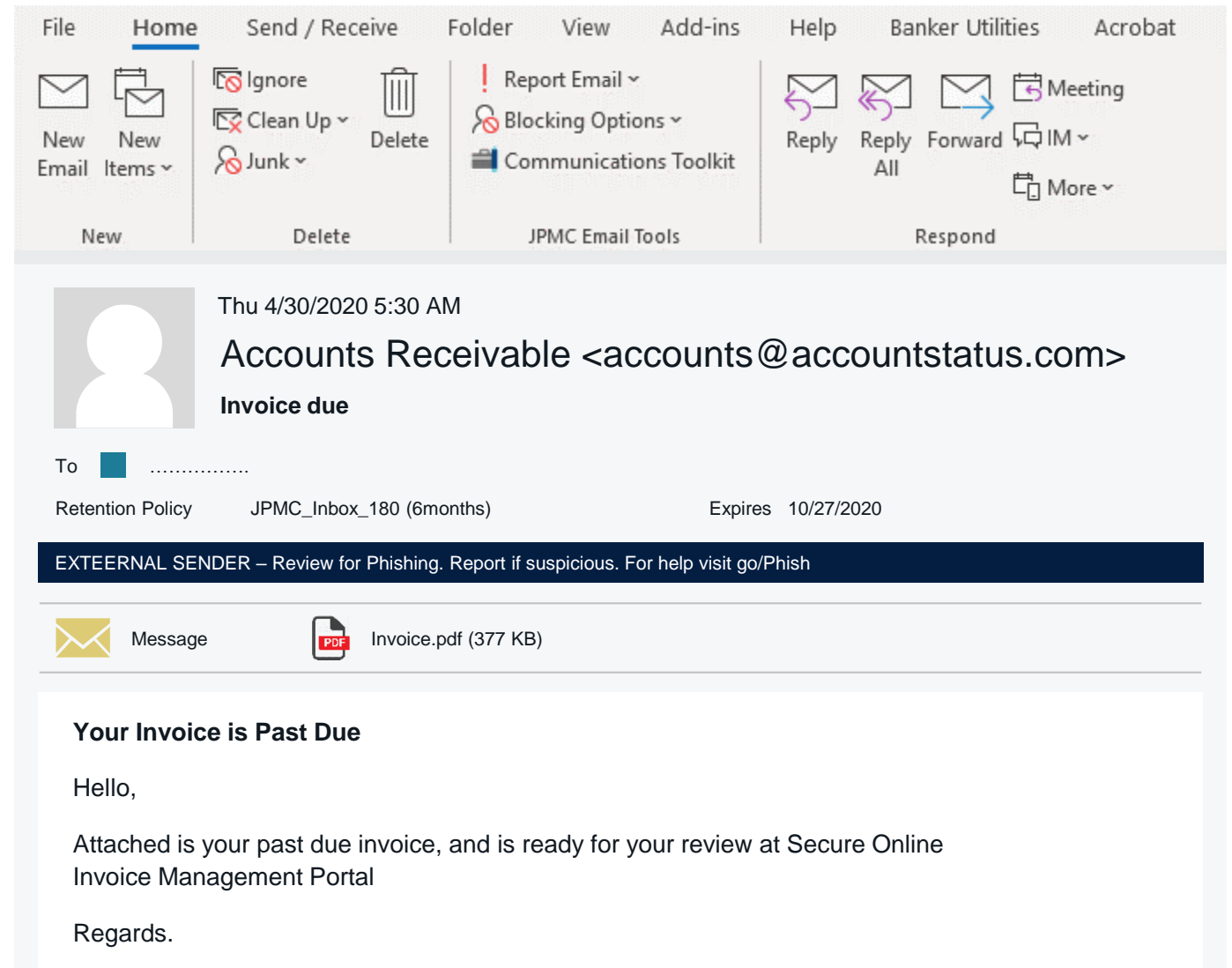
Phishing indicators

 **\$18,728,550**

In losses reported to FBI in 2023¹

- Sender name is vague or generic
- Sender address has a suspicious domain
- Email includes an external banner indicating it's coming from outside the company
- Urgent or authoritative language
- Demands for a quick response
- PDF attachment "View File" button in a link, not a PDF

¹ 2023 FBI IC3 Report



The screenshot shows an Outlook email interface. The ribbon at the top includes 'File', 'Home', 'Send / Receive', 'Folder', 'View', 'Add-ins', 'Help', 'Banker Utilities', and 'Acrobat'. The 'Home' ribbon is active, showing 'New Email', 'New Items', 'Ignore', 'Clean Up', 'Junk', 'Delete', 'Report Email', 'Blocking Options', 'Communications Toolkit', 'Reply', 'Reply All', 'Forward', 'Meeting', 'IM', and 'More' buttons. The email header shows the sender as 'Accounts Receivable <accounts@accountstatus.com>' with the subject 'Invoice due'. The email body contains a warning banner: 'EXTERNAL SENDER – Review for Phishing. Report if suspicious. For help visit go/Phish'. Below the banner, there is a message icon and a PDF attachment named 'Invoice.pdf (377 KB)'. The main text of the email reads: 'Your Invoice is Past Due', 'Hello,', 'Attached is your past due invoice, and is ready for your review at Secure Online Invoice Management Portal', and 'Regards.'

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 use 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

Who are “they”?

Motivated by political, economic, military or ideological objectives

Nation-State Threat Actor

- People or groups who facilitate
 - Hacking
 - Sabotage
 - Theft
 - Disinformation
- Against
 - Other nations
 - Organizations
 - Critical infrastructure



Countermeasures to Nation-State cyber attacks

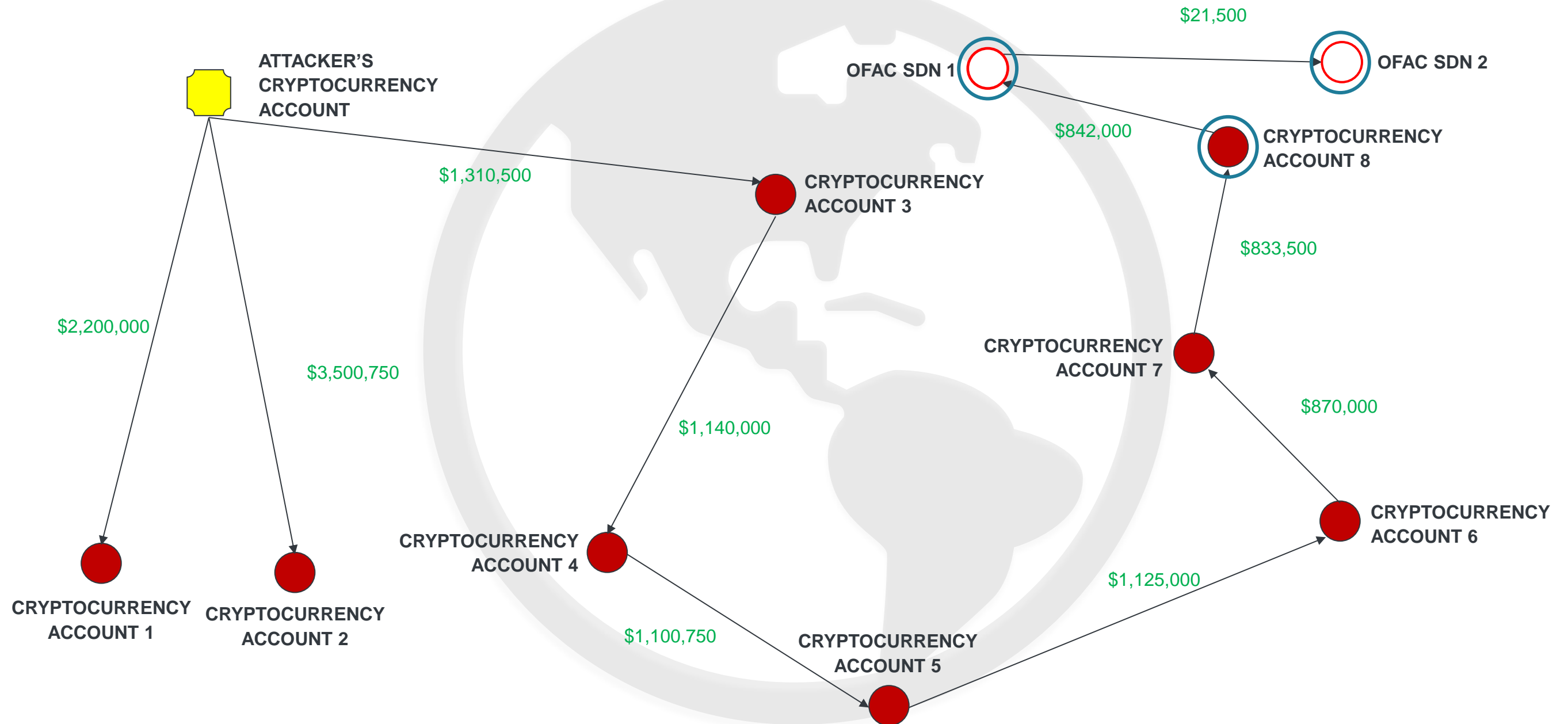
Multi faceted approach: Government, law enforcement and private sector

1. International cooperation and info sharing
2. Robust cyber policies
3. Enhanced attribution facilitates forensics and appropriate response
4. Deterrence establishes consequences and shapes rules of engagement in cyberspace
5. Ongoing education and awareness



Ransomware chain of custody

Careful orchestration of each stage of attack, from infiltration and encryption to negotiation and receipt of payments while avoiding law enforcement intervention




Quantum computing

Cutting-edge technology utilizing the principles of quantum mechanics to solve complex problems more efficiently than standard computers.

- Faster problem solving
- Enhanced data analysis
- Breakthroughs in cryptography
- Optimization and resource allocation
- Accelerated drug discovery
- Advanced machine learning

Quantum computers are **158 million times faster** than the most sophisticated supercomputers²

Can also pose threats.

- Encryption vulnerabilities
- Data breaches
- Cryptography
- Authentication and access control
- Digital signatures
- Phishing and social engineering 

Leading experts believe quantum computers can crack public-key cryptosystems **within a mere 24 hours**³

Expected Growth

 **\$6.9B**

Projected quantum computing market value by 2030⁴

 **\$1.3T**

Potential economic value from quantum computing by 2035¹

¹ McKinsey & Company, *Quantum Technology Monitor*, April 2023

² LiveScience, *Quantum computing: Definition, facts & uses*, 2022

³ IBM Institute for Business Value, *Security in the quantum computing era*, 2023

⁴ Quantum Computing Market, *Information Technology – Market Research Report*, February 2024

What to expect when check fraud happens

Overview of the resolution process



1 | Claim is reported

The client informs the bank and reports a claim



2 | Documentation is provided

The client provides the required documentation to Chase



3 | Investigation

Back-of-check fraud

Chase makes a claim on the bank where the check was deposited

- **If deposited at a Chase bank**, it could take up to 15-20 business days if all the required documents have been provided
- **If the bank was not Chase**, it could take six months or more
- We reach out to the other banks with the claim; however, they control the response time frame

Mobile Deposit Fraud

Chase makes a claim on remote deposit capture bank

- **If deposited at a Chase bank**, it could take up to 15-20 business days if all the required documents have been provided
- **If the bank was not Chase**, it could take up to 30 business days
- We reach out to the other bank with the claim; however, they control the response time frame

Front-of-check fraud or counterfeit

- Internal Chase investigation could take up to 15-20 business days if all the required documents have been provided

Other reasons your claim could be delayed

- The depositing bank could ask for more documentation such as W-9 forms, tax documents, police report, driver's license or a payee-signed affidavit.
- The case could also involve an altered check or dual payees



4 | Resolution

The claim is paid or denied. If there is a request for more information, then you must go back to Step 3.

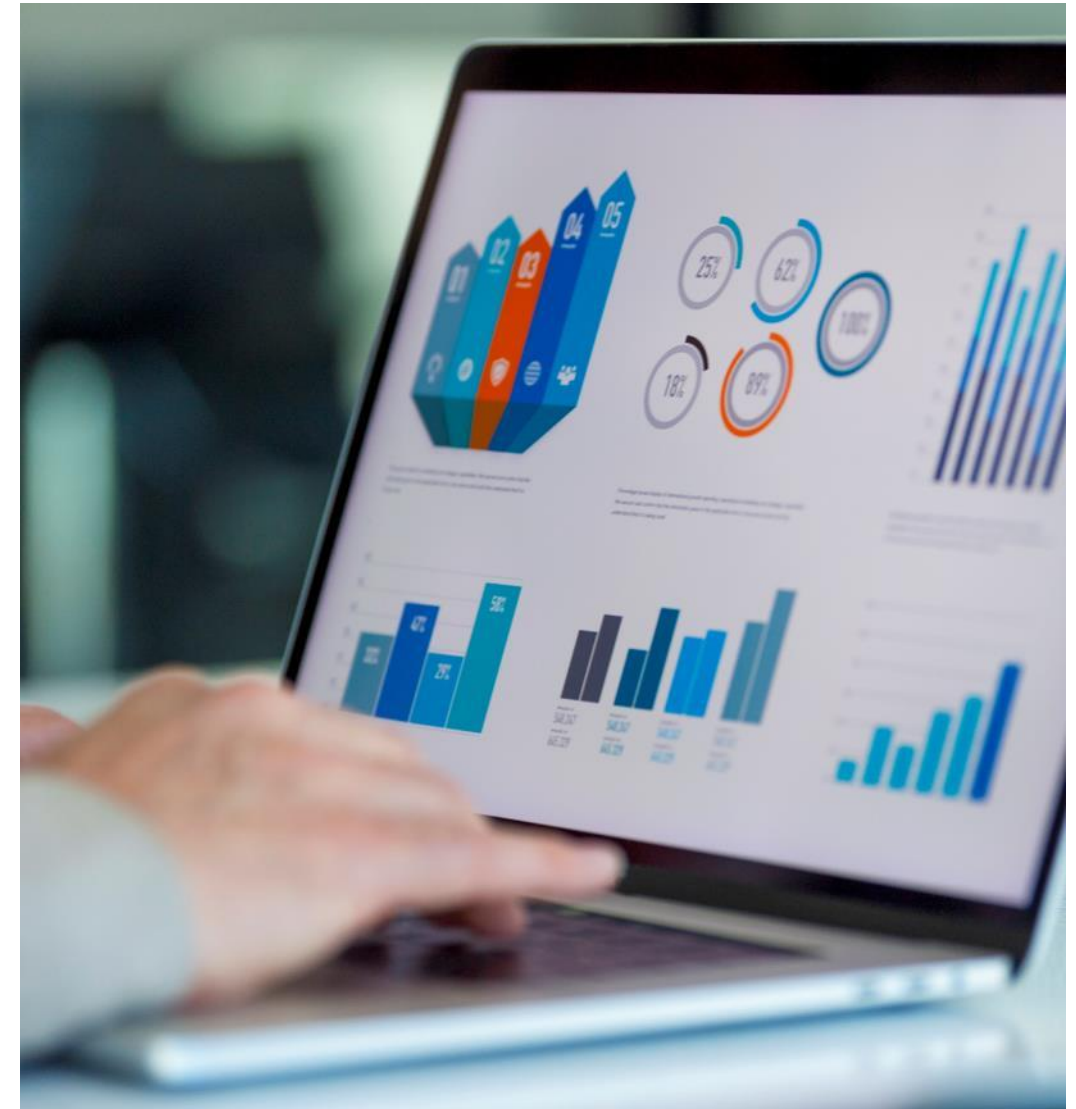
Cyber budget

ROI:

\$ Monetary +
Non-Monetary

What is Optimization

- Overlapping solutions
- Outdated security configurations (especially in cloud)
- Update software and hardware
- Underspend on critical elements
- Overspend
- Rationalize and deprecate to reduce bloat
- Actual legacy costs, maintenance, plus security
- All data is not created equally
- Well known tools have well known weaknesses



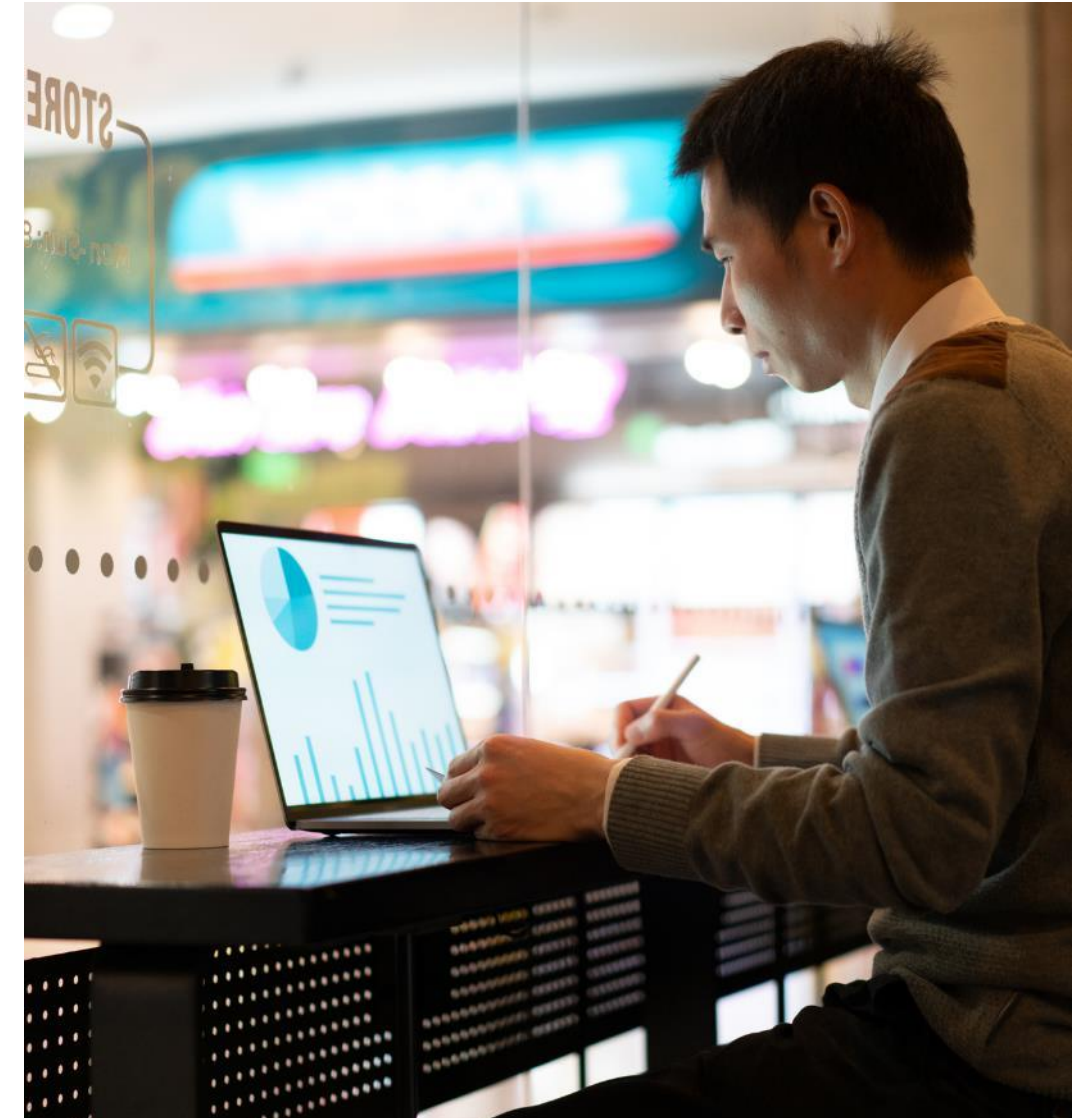
Cyber budget optimization

\$5.13M

Average cost of a ransomware attack,
not including the ransom itself

“How to”

- Best vs Effective/Right Size
- CISO and CFO collaboration
- Segmentation Sensitive vs Non sensitive
- Understand actual vs perceived threats
- Learn ALL tool capabilities before purchase
- Reduce attack surface
- Regular risk assessments
- MDR/XDR – Active response with alerts
- Develop an ACTIVE Cloud Cyber Strategy

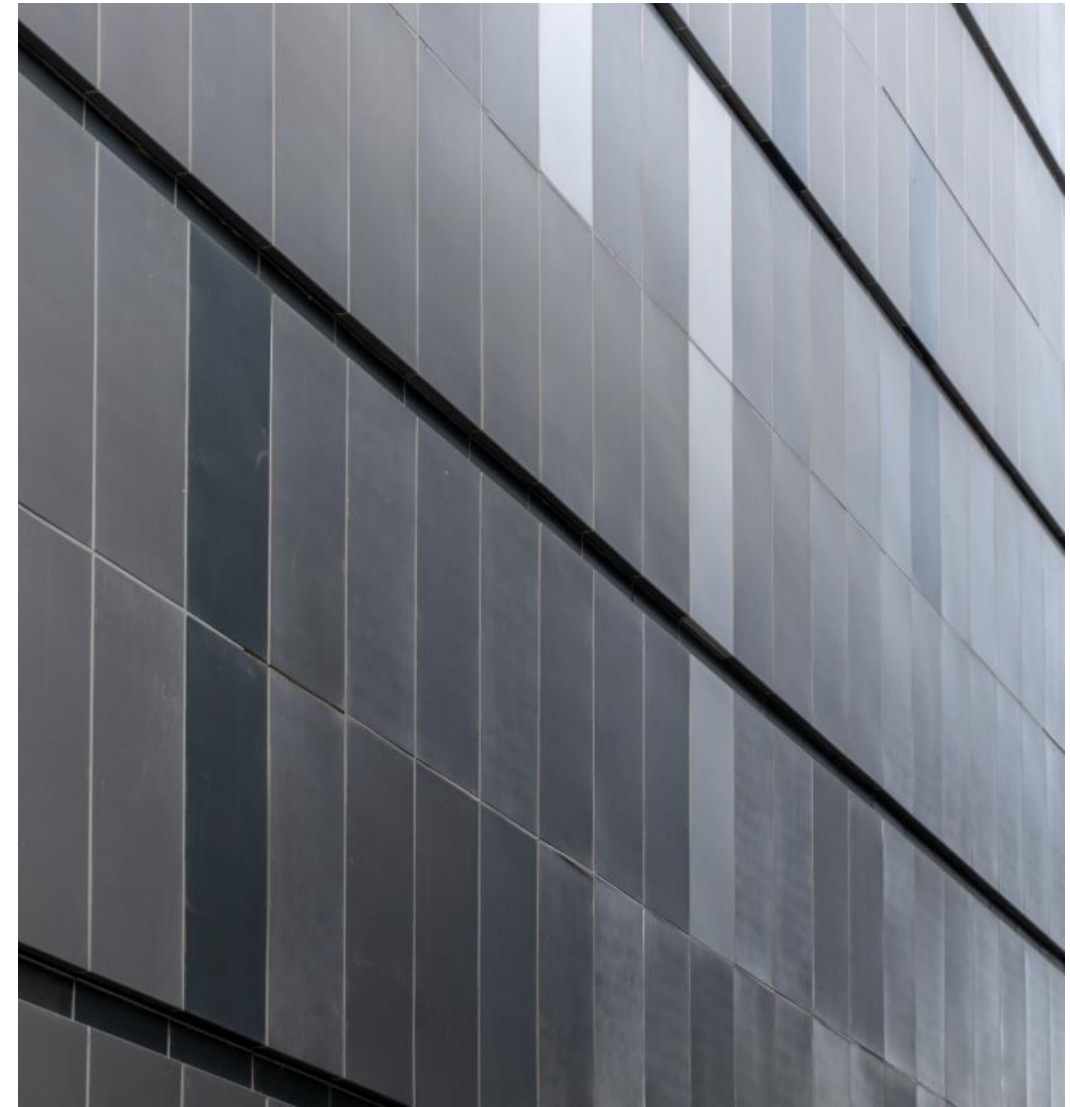


¹IBM Security: Cost of a Data Breach Report 2023

Define and enforce a cybersecurity policy

Key Considerations

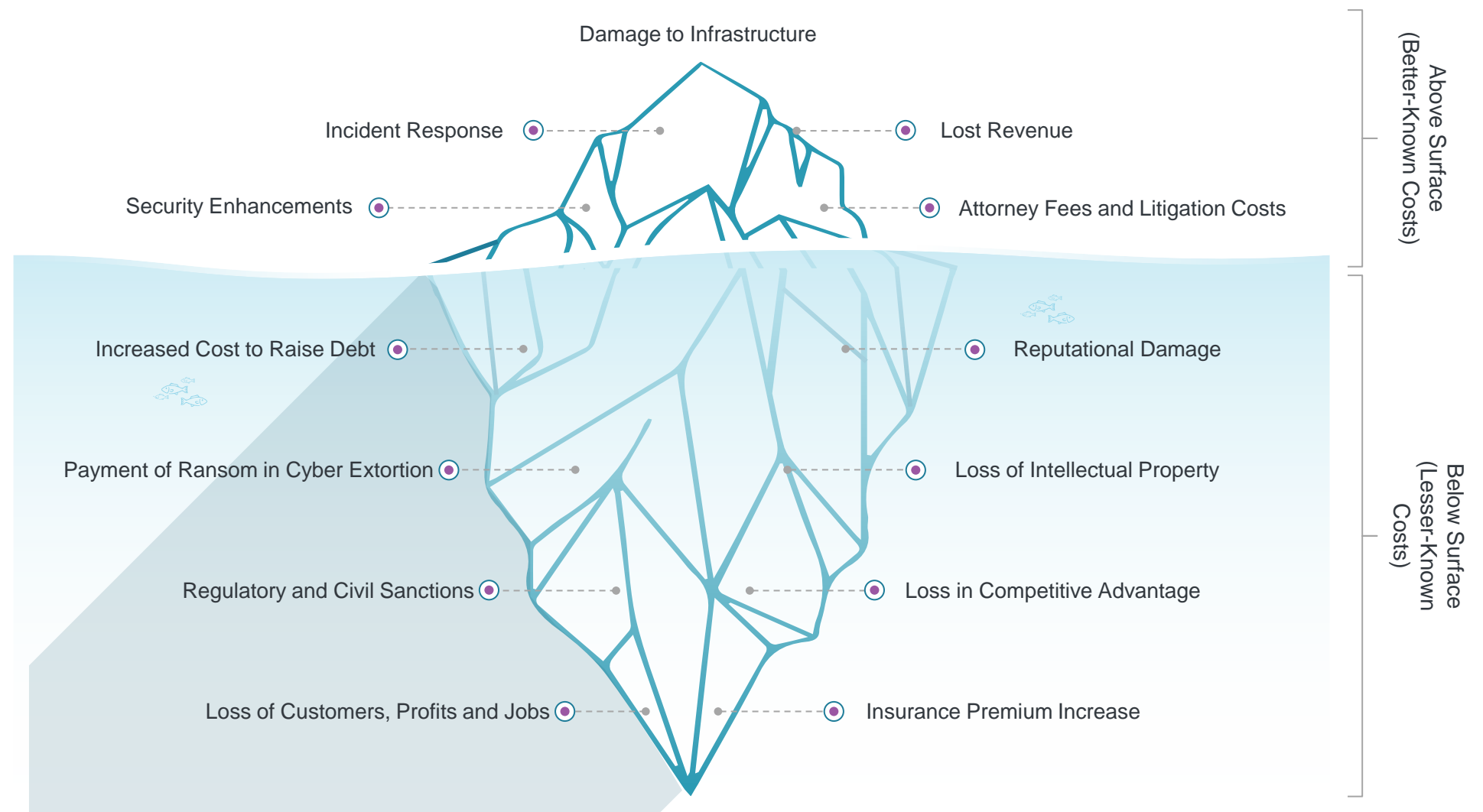
- Data loss prevention standards
- Software updates
- Social media requirements
- Encryption & content sharing
- Employee training
- Network access
- Incident reporting process



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



Disclosures

Chase, J.P. Morgan, 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 Commercial Banking affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those that can be provided by Commercial 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 Commercial 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/global/disclosures/interbank_offered_rates.

JPMorgan Chase Bank, N.A. Member FDIC.

© 2024 JPMorgan Chase & Co. All rights reserved.