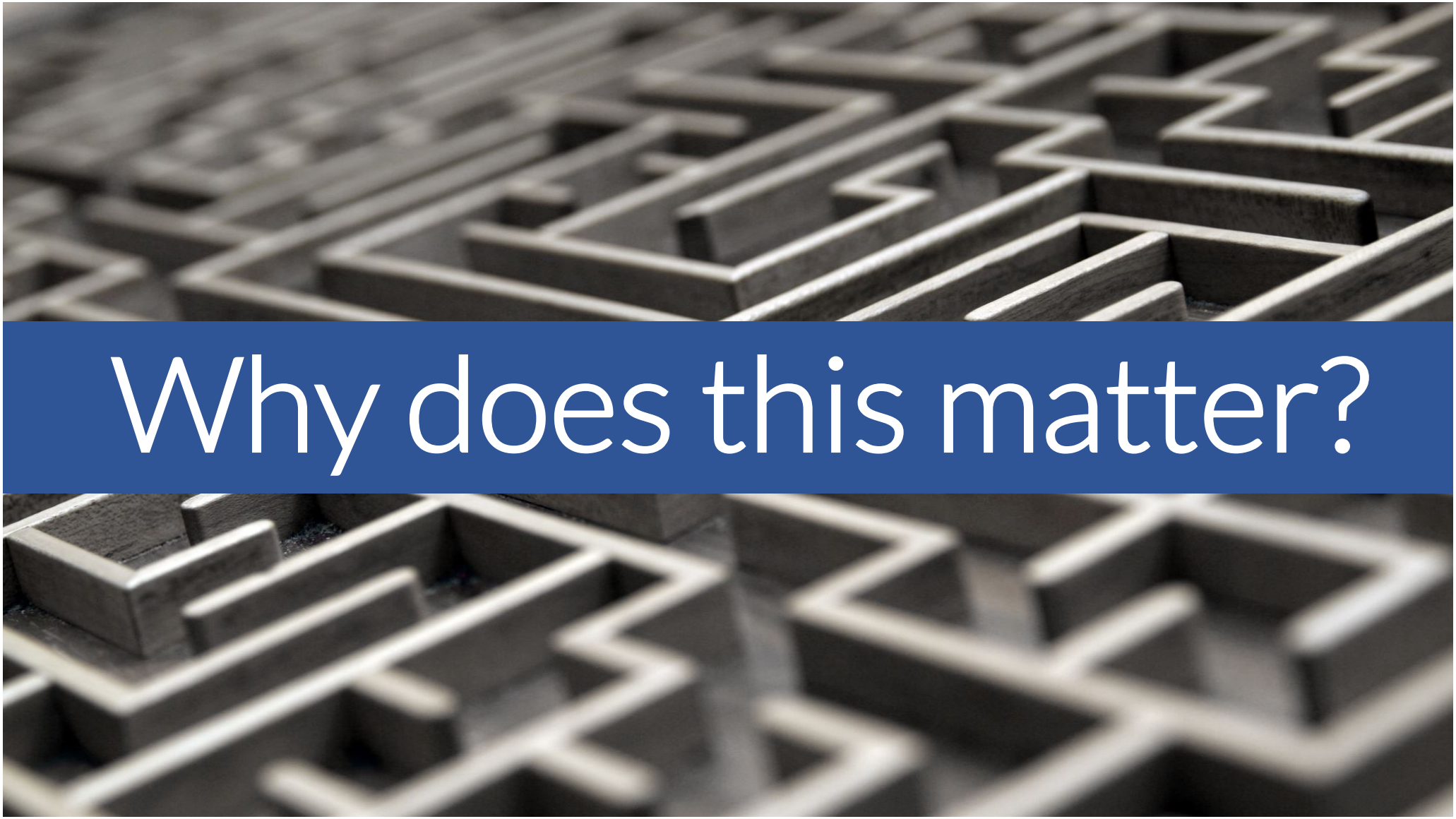
The Ever-Changing Threat Landscape in Banking

Trends, Forecasts, and AI's Role

BEDEL security | www.bedelsecurity.com | (833) 297-7681 | support@bedelsecurity.com



Why does this matter?

Trend:

"The disparity between the banks that thrive and those that merely survive will continue to grow over the next decade and will be dependent on the level with which they choose to embrace technology."

FIGURE 8

How important are the following internal risks facing your bank today?

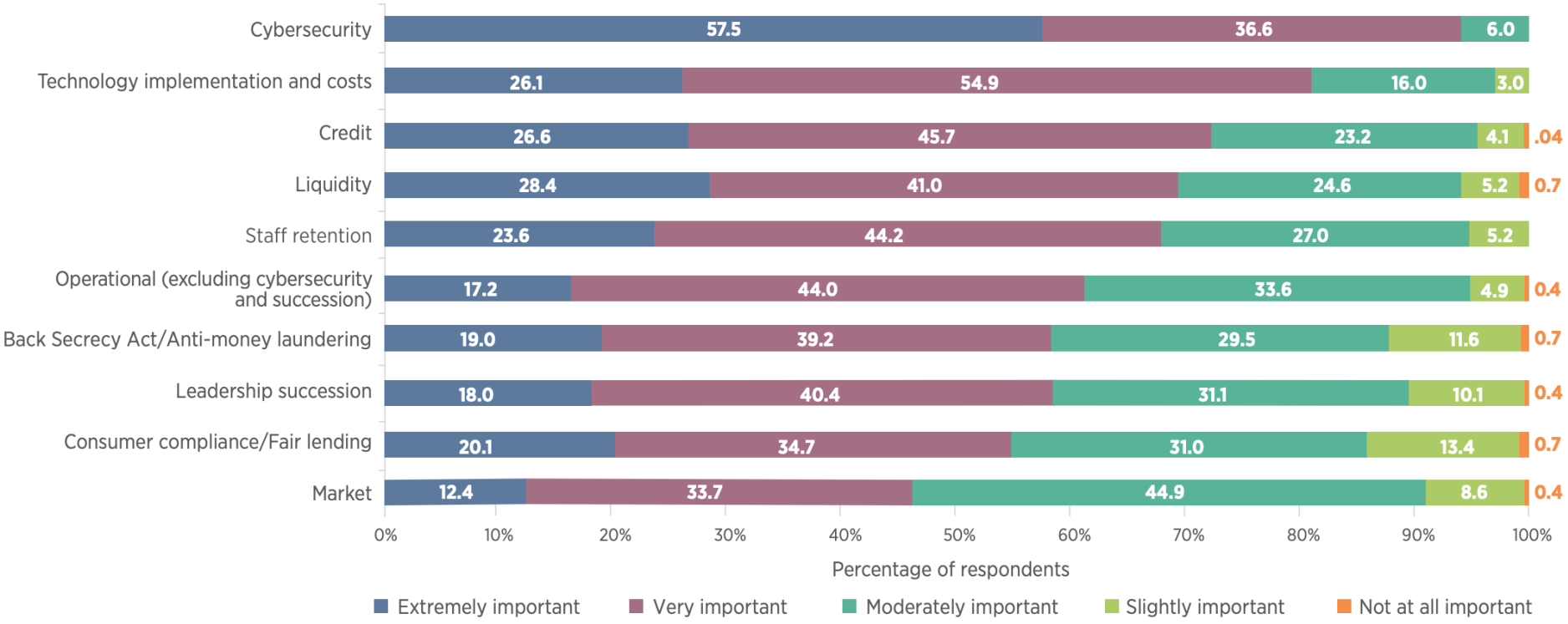
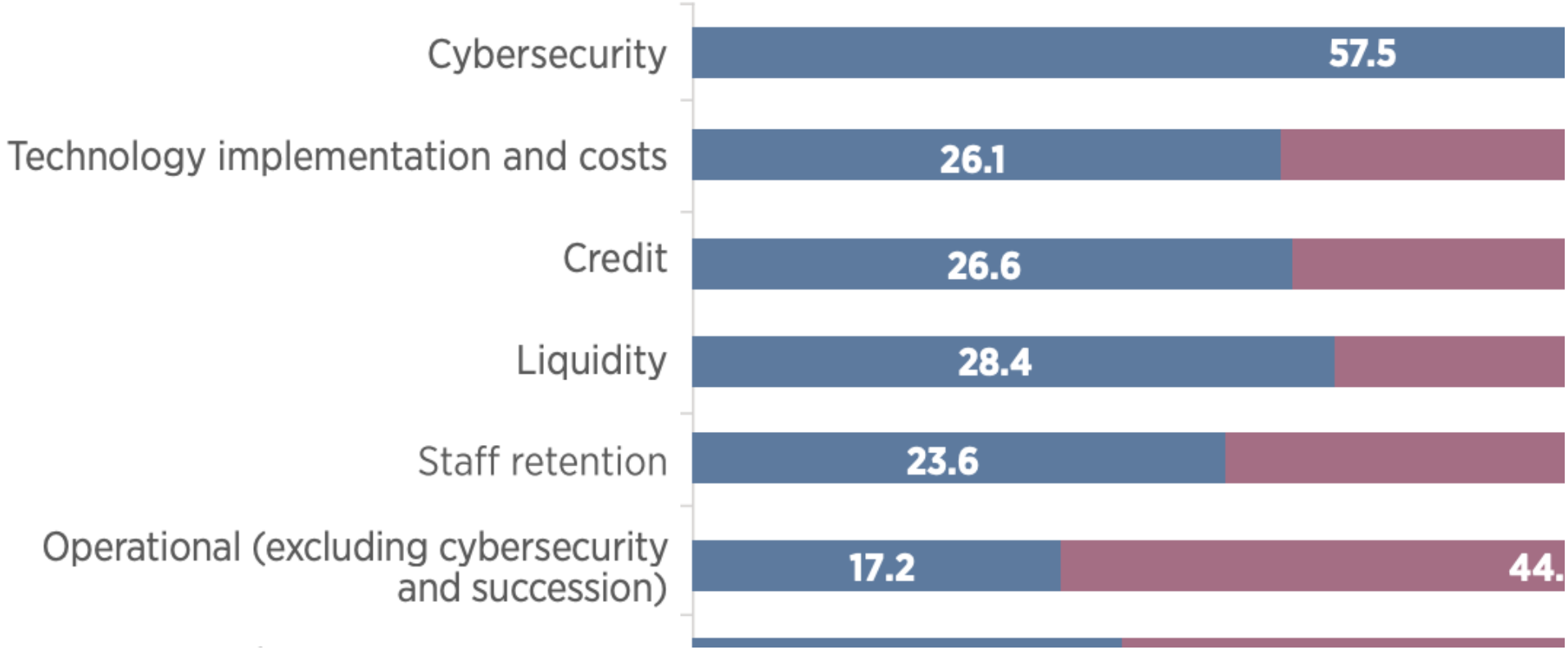


FIGURE 8

How important are the following internal risks facing your bank toda



What we'll talk about

-Business Email Compromise (still)
-Artificial Intelligence
-Deepfakes
-Old and New Threats
-What you can do!

About Bedel Security

- Founded in 2015
- Focused entirely on Virtual CISO offering
- Exclusively work with community financial institutions
- Using our proprietary CySPOT™ platform
- Clients from Boston to Seattle; from Houston to Bismarck
- Clients ranging in size from $45MM in assets to over $9 Billion

Business Email Compromise

BEDEL security | www.bedelsecurity.com | (833) 297-7681 | support@bedelsecurity.com

FDIC Chicago Region
IT, Security, and Cybersecurity Risk Response Report (3Q and 4Q 2024)

Risk	Prev. Rank	Level / Direction	Response	Commentary
Account Takeover/ E-mail Compromise (Social Engineering, Phishing, Malware, and Web Application Attacks / Website Spoofing)	#1	Moderate / ↑ (eight instances vs. five prior)	• IT governance: responsibilities, threat intelligence processes, information security/cybersecurity (IS/CS) assessments, policies, and reports • Vendor management: risk assessments, policies, due diligence and ongoing oversight reviews, and reports • Strategic planning: training/awareness programs (including customers) • Configuration management: access controls (including multi-factor authentication, privileged account management, and least privilege); application security (i.e., account authorizations, device registration, authorized IP addresses, out-of-band verifications, and transaction limits); firewall/router/switch configurations (i.e. whitelisting); and operating system (OS) hardening • Patch management: continuous vulnerability assessment and remediation processes for devices, applications, and OSs • Malware defense: anti-virus and anti-spyware	Coordinated attacks/impersonations (including via bank communications and text messages), spear-phishing, and social engineering are evident. Multi-factor authentication, application security, account monitoring, and employee and customer education programs are relevant mitigating controls. Attackers continue to target accounts maintained outside the institution (i.e. Internet banking/P2P applications, payroll, and e-

ABA BANKING JOURNAL
From the American Bankers Association

OCC publishes letter with details about agency data breach

April 15, 2025 Reading Time: 1 min read

Artificial Intelligence

Now (2025)

- Threat Detection
- Fraud Detection
- Meeting Minutes
- Marketing copywriting / brainstorming
- Chatbots
- Coding
- Credit Decisioning (!)
- AI-generated AI

BBC

AI system resorts to blackmail if told it will be removed

23 May 2025

Share Save

Liv McMahon
Technology reporter

BBC

AI firm says its technology weaponised by hackers

28 August 2025

Share Save

Imran Rahman-Jones
Technology reporter

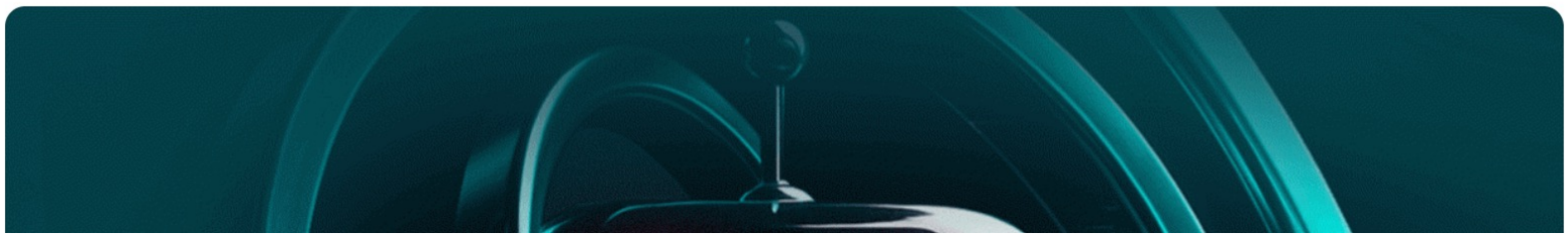
Digital Security

AI-aided malvertising: Exploiting a chatbot to spread scams

Cybercriminals have tricked X's AI chatbot into promoting phishing scams in a technique that has been nicknamed "Grokking". Here's what to know about it.

Phil Muncaster

13 Oct 2025 • 5 min. read



Trend:

AI won’t replace you in your job…

… someone who uses AI will.

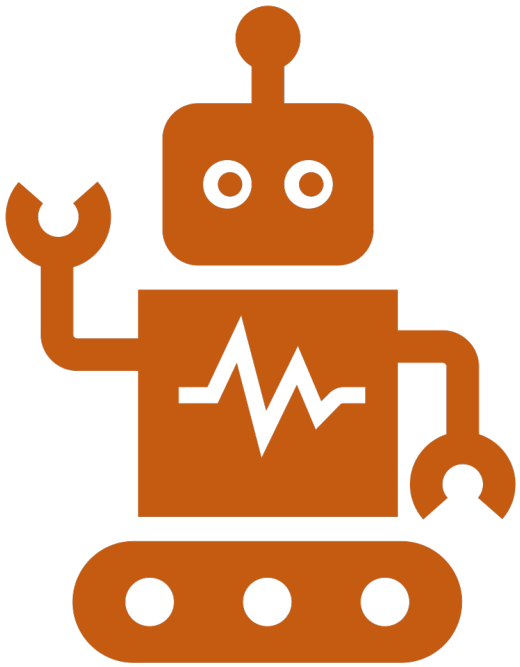
UPTIQ Products Platform Solutions For Resources

Real AI

The AI Platform for Financial Services

Outcome-driven AI agents that drive growth, scale operations, and deliver results across banks, credit unions, wealth, fintech, and non-bank lenders.

3 Year (2028)



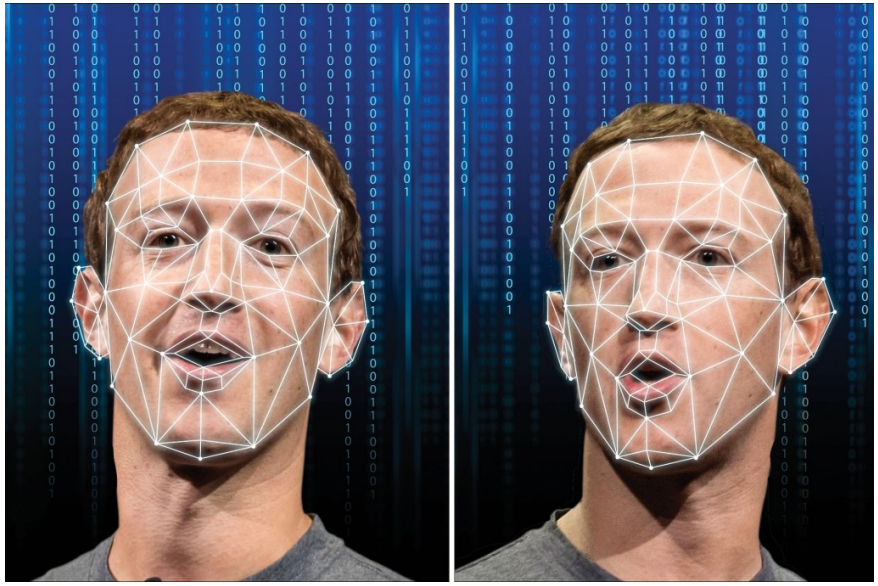
- AI achieves human intelligence (AGI)
- Integration into almost every application you use – including banking
- Enhanced risk management
- Humanoid robots in manufacturing, service, homes
- Robotaxis prevalent
- Threat actors will continue to exploit these resources!

Trend:

Deepfake audio attacks will be the next big wave of social engineering to hit the banking industry.

Deepfakes

- Video and **Audio**
- Getting easier and better
- How are you verifying your customers? Your employees?



What are the internal risks of AI?

- GLBA/Confidential data exfiltration
- GLBA/Confidential data used to train LLMs
- Biases in decision making (Credit/Lending)
- Hallucinations
- Shadow IT
- Technical Atrophy

If AI is not for you:
(or not right now)

- Risk Assessment (light)
- AI Policy
- Train your people
- Block sites in webfilter/DLP
- Check with your vendors

If you choose to implement AI

- Form a committee
- Risk assess (deeper)
- Policy
- Tell your examiners
- Enterprise Copilot
  - Test configurations
  - Test permissions
- Train your people

Trend:

Criminals don’t care what the attack is, as long as it profitable. That means they’ll re-use attacks when we let our guard down.

ATM jackpotting attacks have increased

SafeAlert™

Printable pdf: SafeAlert ATM Jackpotting Attacks Have Increased-SA27

Criminals are using master keys and endoscopes to get into ATMs.

ATM attacks have been rampant since 2018 and are showing no signs of letting up. For several years, “hook and chain” attacks were the most common method of ATM theft. To mitigate risk of this type of theft, many banks erected physical barriers.

More recent incidents, however, involve individuals using generic or master keys to unlock a machine’s exterior chassis or endoscopes to get inside an ATM. No trucks required.

Shockingly, these can easily be purchased on the internet. The criminals then tamper with the machine’s hard drives to install malware, ultimately resulting in the disbursement of cash. This is known as ***“jackpotting”—altering the ATM mechanisms and typically inserting malware, to cause the machine to dispense cash to unauthorized users.***

The U.S. Secret Service has reported an increase in ATM jackpotting over the last six months. The attacks are believed to be the work of organized criminal groups and target multiple ATM manufacturers.

Public Service Announcement

FBI & USPIS

Alert Number: I-012725-PSA
January 27, 2025

Mail Theft-Related Check Fraud is on the Rise

The FBI and USPIS are warning that check fraud is on the rise, with a significant volume enabled through mail theft. Suspicious Activity Reports related to check fraud have nearly doubled from 2021 to 2023.[1] Fraudsters take advantage of regulations requiring financial institutions to make check funds available within specified timeframes, which is often too short a window for the consumer or financial institutions to identify and stop the fraud. As a result, the compromised checks clear, and the funds are withdrawn by the criminal participants before the fraud is detected.

Trend:

The threat of nation state actors will continue to increase in the coming years.

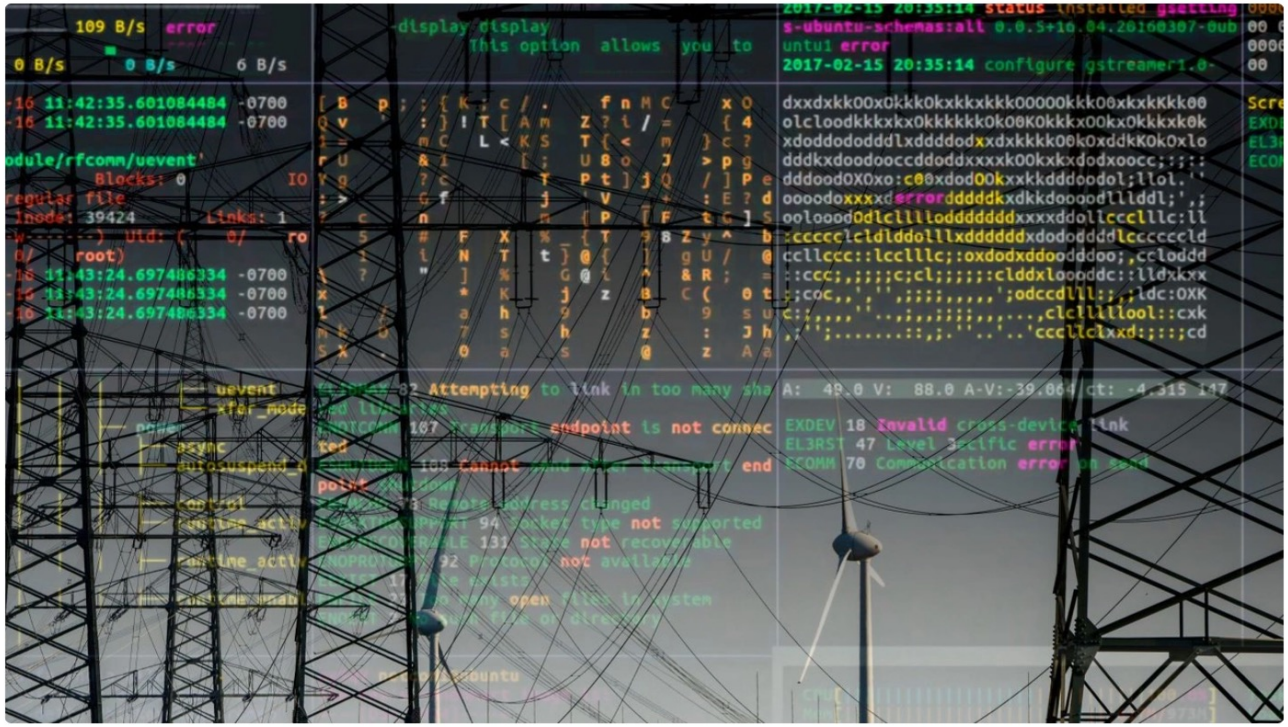
Volt Typhoon Strikes Massachusetts Power Utility

The prolonged attack, which lasted 300+ days, is the first known compromise of the US electric grid by the Voltzite subgroup of the Chinese APT; during it, the APT attempted to exfiltrate critical OT infrastructure data.

Elizabeth Montalbano, Contributing Writer

March 12, 2025

3 Min Read



SOURCE: JOCHEN TACK VIA ALAMY STOCK PHOTO


What do we do about it?

The 6 Mistakes in Cybersecurity

1. Disengaged leadership
2. In the weeds
3. Unwilling to invest in IT
4. Unsure what “good” looks like
5. Inexperienced information security officer
6. Lack of independence

Mistake #1: Disengaged Leadership

"Cybersecurity? That's IT's problem"

"We only had a few findings on our exam, so we must be good"

"You can look into rolling that out after I retire in a couple of years"

Mistake #2: Getting Into the Weeds

Obsessing over the “threat of the day”

Buzzword fixes (Zero Trust, AI, etc.) without foundation

Very **reactionary** – without big picture

Mistake #3: Not Investing in IT

You can't secure weak IT infrastructure

Risk: stalled programs, frustrated staff

This is your frontline defense

Mistake #4: Not Knowing What 'Good' Looks Like

It's hard to govern what you can't define.

Collectively, we must build this muscle memory.

GLBA Report

- Policies
- Strategic Plan
- Business Continuity
- Audit & Exam
- Risk Assessments
- Incident Response
- Cyber Framework (CSF)
- Third Party Due Diligence
- Cyber Insurance
- Employee Training
- Social Engineering Testing
- Vulnerability Management
- Risk Appetite Statement
- Overview & Summary

Mistake #5: Inexperienced ISO

Has no desire to be ISO

Has the desire, but lacks the knowledge and expertise

Compliance

Strong familiarity with bank IT regulatory requirements; experience in working with IT auditors and examining agencies

Information Systems

Knowledge of and experience with networking, servers, applications, and other bank-specific systems

Cyber Threats and Security

Understanding of threat actors, motives, techniques, and compensating controls to combat such attacks

People Skills

Is approachable; can explain complex concepts in plain English; excellent verbal and written communication skills

Business and Banking Experience

Takes a business-enablement approach to security; has direct banking experience to appreciate unique challenges of the industry

Risk

Can identify and prioritize threats and vulnerabilities based on likelihood and impact of a given event; can create action plan to implement mitigating controls

Mistake #6: Lack of Independence

IT and Security ≠ same role

IT = innovation, speed | Security = brakes, caution

Healthy tension is required

Independence now flagged by examiners

Role	Should NOT be doing
CISO, ISO, or Security Leadership	IT Leadership (CIO), IT Support, IT Networking, IT Administration, Core Banking, Audit, Pen Testing, Monitoring
IT Dept. or Managed IT Vendor	ISO, CISO, IS Leadership, Pen Testing, Audit
Core Provider	ISO, CISO, IS Leadership, Pen Testing, Audit
Auditor	IT Leadership (CIO), IT Support, IT Networking, IT Administration, Core Banking, Monitoring, ISO, CISO, IS Leadership

Tips to avoid the 6 mistakes:

1. Ask the right questions
2. Stay at a strategic level
3. Invest in IT
4. Expect a repeatable security program
5. Work with an experienced Information Security Officer
6. Ensure independence

Questions?

Chris Bedel, CISM

812-552-2258 x700

chris@bedelsecurity.com

Our Book:
https://www.bedelsecurity.com/bos-book