2023 OACTFO Conference

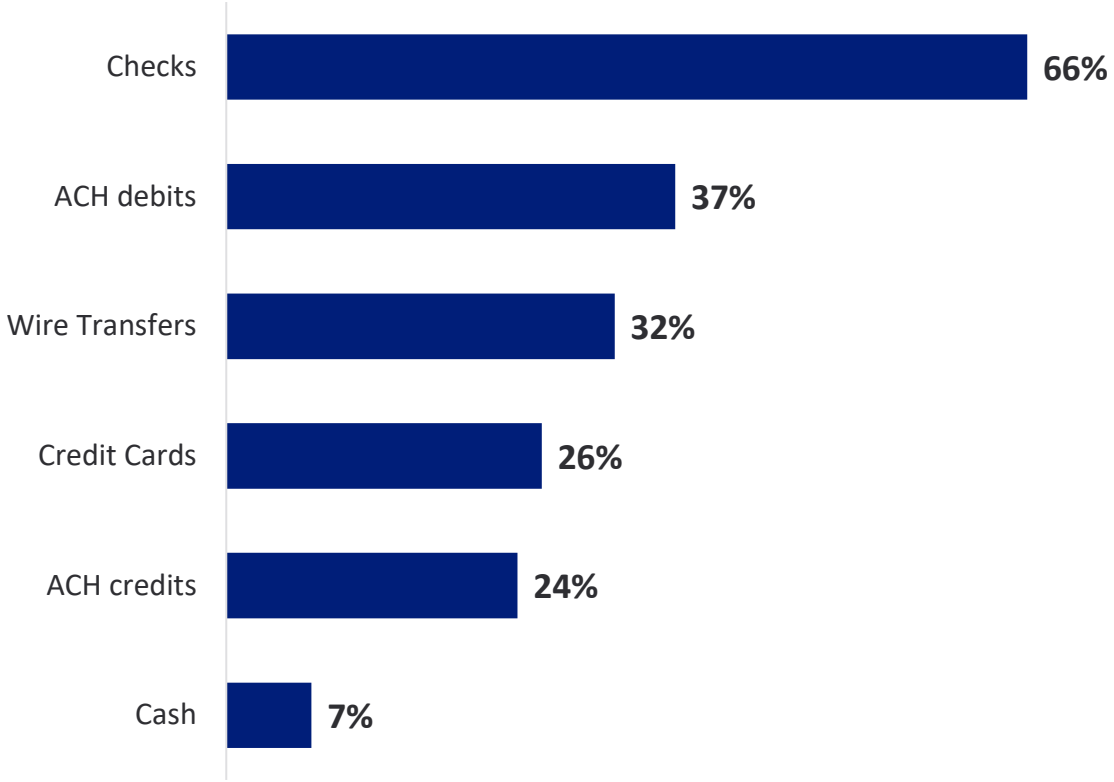
Fraud and Data Security

Protecting payments, Data and People in the office and remotely

Jim Stamm and Anne Adriano

Payment fraud in 2021

Payment methods subject to attempted/actual payment fraud (percent of organization)



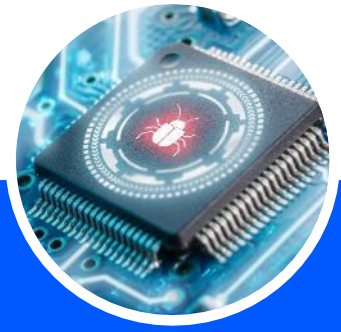
Source: AFP® 2022 Payments Fraud & Control Report.
Note: Percent of organizations that experienced attempted and/or actual payments fraud in 2020.
2023 AFP Payments Fraud and Control Survey (afponline.org)

Checks and ACH continued to be the payment methods most impacted by fraud activity.

Be aware of increasing cybersecurity threats

Business Email Compromise (BEC)

A scam where the fraudster spoofs or masquerades as a business email account in order to access the company and perform fraudulent transactions.



Malware

Any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems (i.e., Email Account Compromise).

Ransomware

A type of malware that restricts access to the system (operational access) which deters an organization from business as usual until unlocked or encrypts sensitive data and does not allow for data to be unencrypted until ransom is paid.

How criminals carry out business email compromises (BEC) scams

Spoof an email account or website

BEC attackers pose as a person or entity that a recipient can trust, such as a colleague, boss or vendor.

Send spear phishing emails

The attacker sends an email directing recipient to take some action that siphons money or sensitive financial information from the organization. These could include fraudulent wire transfers, bogus invoices, diverted paychecks, changed banking details for future payments and other schemes.

Often too late

By the time the organization discovers the error, it is often too late to recover the money.

Source: IC3 Annual Report: https://www.proofpoint.com/us/resources/e-books/definitive-email-security-strategy-guide

From: Sally.Smith@amycompany.com
To: Jeff Anderson
Subject: FWD: Payment to ABC Client

Jeff,

Need this processed immediately. Thanks.

Sally

---Begin Forwarded Message---
From: Bob.Jones@anycompany.com
Sent: Wednesday, April 16, 2015 3:40 PM
To: Sally.Smith@amycompany.com
Subject: Payment to ABC Client

Sally,

ABC Client called me personally this morning and is fairly upset at us. Need your team to complete the wire they asked for multiple times. Please transfer $151,023 from my admin to 12345678 acct 78910100 as soon as possible.

Bob
Sent from my iPhone.

Example of a spoofed email

From: **Sally.Smith@amycompany.com**
To: Jeff Anderson
Subject: FWD: Payment to ABC Client

Jeff,

Need this processed immediately. Thanks.

Sally

---Begin Forwarded Message---
From: **Bob.Jones@anycompany.com**
Sent: Wednesday, April 16, 2015 3:40 PM
To: **Sally.Smith@amycompany.com**
Subject: Payment to ABC Client

Sally,

ABC Client called me personally this morning and is fairly upset at us. Need your team to complete the wire they asked for multiple times. Please transfer $151,023 from my admin to 12345678 acct 78910100 as soon as possible.

Bob
Sent from my iPhone.

Take a careful look at how they manipulate email addresses

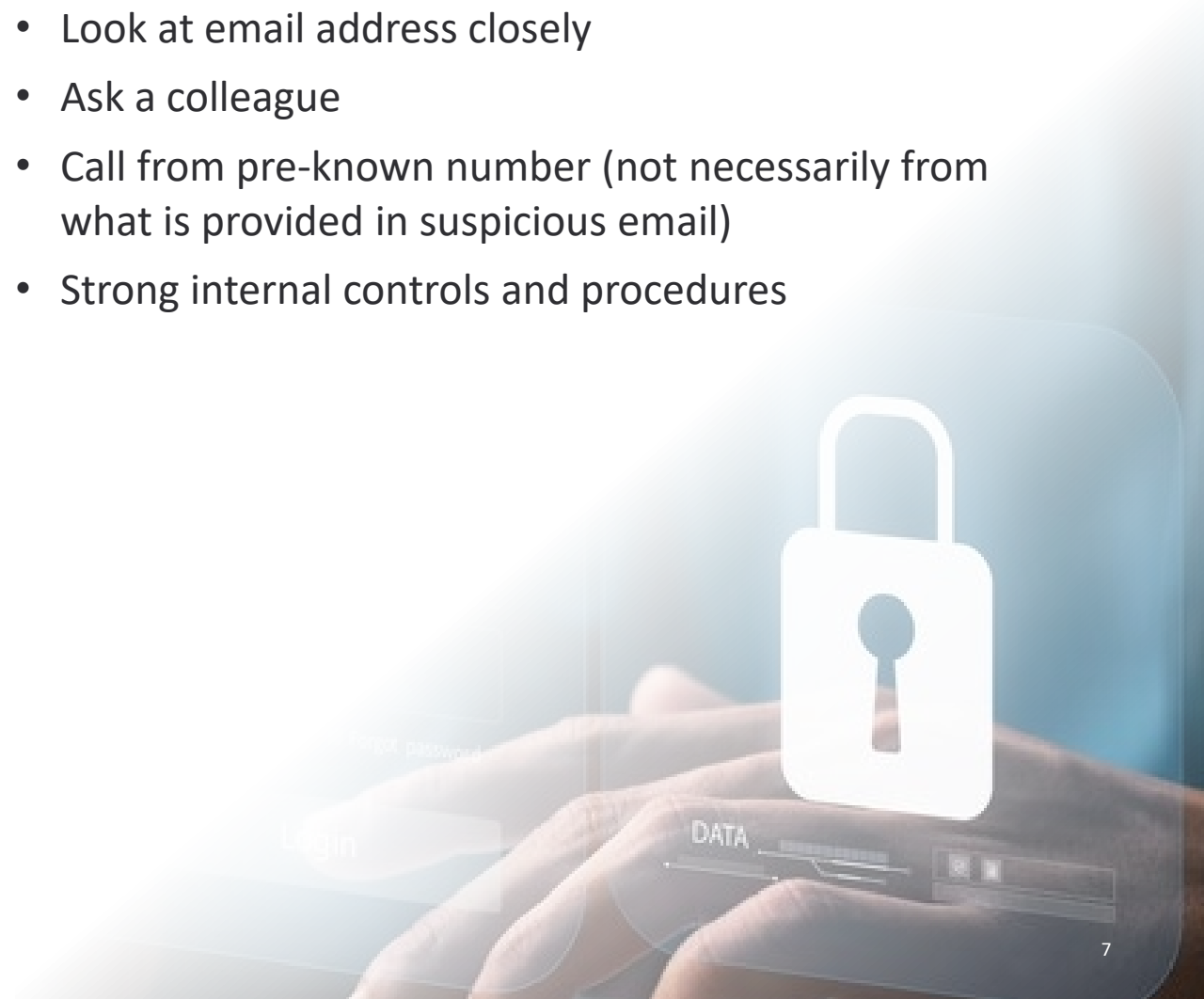
BEC Watchlist cheat sheet

What to watch for:

- Asking for a receipt/confirmation
- Let me introduce you to…
  - Setting up a check-in/quarterly meeting (i.e., pulse check)?
- Switching from email to alternate communication (e.g., SMS)
- Vulnerable time for customer
  - Going through change/merge/onboarding/new bank relationship change.
  - Holidays/busy times
  - New staff
  - Monday, Friday
  - Thematic events (e.g., seasonality, international unrest/conflict, health crisis.)

What to do:

- Look at email address closely
- Ask a colleague
- Call from pre-known number (not necessarily from what is provided in suspicious email)
- Strong internal controls and procedures



Thread hijacking red flags

- **Time:** When was the last time you were contacted by this person?
- **Context:** Does the email make sense with the rest of the conversation?
- **Fake Domain:** Domain may be off by a letter or two (e.g. - .com vs .net)
- **Content:** Are you being asked to do something you have never done before? e.g., enter a password to open attachment
  - Are you being asked to perform a high-risk transaction?
  - Look for inconsistencies in email threads:
    - Does the email thread make sense? Sometimes a threat actor can “hijack” an email thread and insert themselves into an already existing thread.
    - Be cautious of older email threads with requests that don’t seem to align with the original thread.

A deeper look at ransomware

- Ransomware renders files and systems unusable until ransom demands are met.
- Ransomware incidents can severely impact mission-critical services.
- The impacts of ransomware incidents can prove challenging for organizations large and small.

In 2021, the IC3 received 3,729 complaints identified as ransomware with adjusted losses of over $49.2 million.

Sources: https://www.ic3.gov/media/news/2020/200728.pdf and https://www.ic3.gov/media/news/2020/200707-3.pdf.

Best practices to prevent ransomware incidents

- Don’t open emails from unknown senders or that you aren’t expecting.
- Don’t click on links in messages.
- Avoid opening attachments in messages.
- Don’t give away personal information that could compromise your devices or identity.
- Compliance Training. Spend time to educate your staff.
- Install anti-virus/anti-malware software and keep it up to date.
- Apply patches to all applications and operating systems.
- Don’t browse suspicious sites.
- Don’t respond to pop-up windows instructing you to call a number for support.
- Remember the red flags on slide 8.

Source: https://www.cisecurity.org/newsletter/2021-cyber-hot-topics-ransomware/.

Source: https://www.cisecurity.org/newsletter/2021-cyber-hot-topics-ransomware/.

Best practices if you are a victim of ransomware

- Don’t respond to a ransom note on the screen.
- Seek professional assistance or advise (Bankers, Local Police and your IT).
- Using a separate non-infected device, change passwords on all accounts that were accessed from that device.

Best practices to avoid check fraud

Types of check fraud	Types of fraud control strategies
• Check kiting • Embezzlement • Bad check writing • Abandonment • Forgery • Check abandonment or ‘paper hanging’	• Positive pay • Daily account review and reconcilements • Segregation of accounts • Payee positive pay • Tamper resistant check features • Outsourcing check printing

Source: AFP® 2020 Payments Fraud & Control Report.:

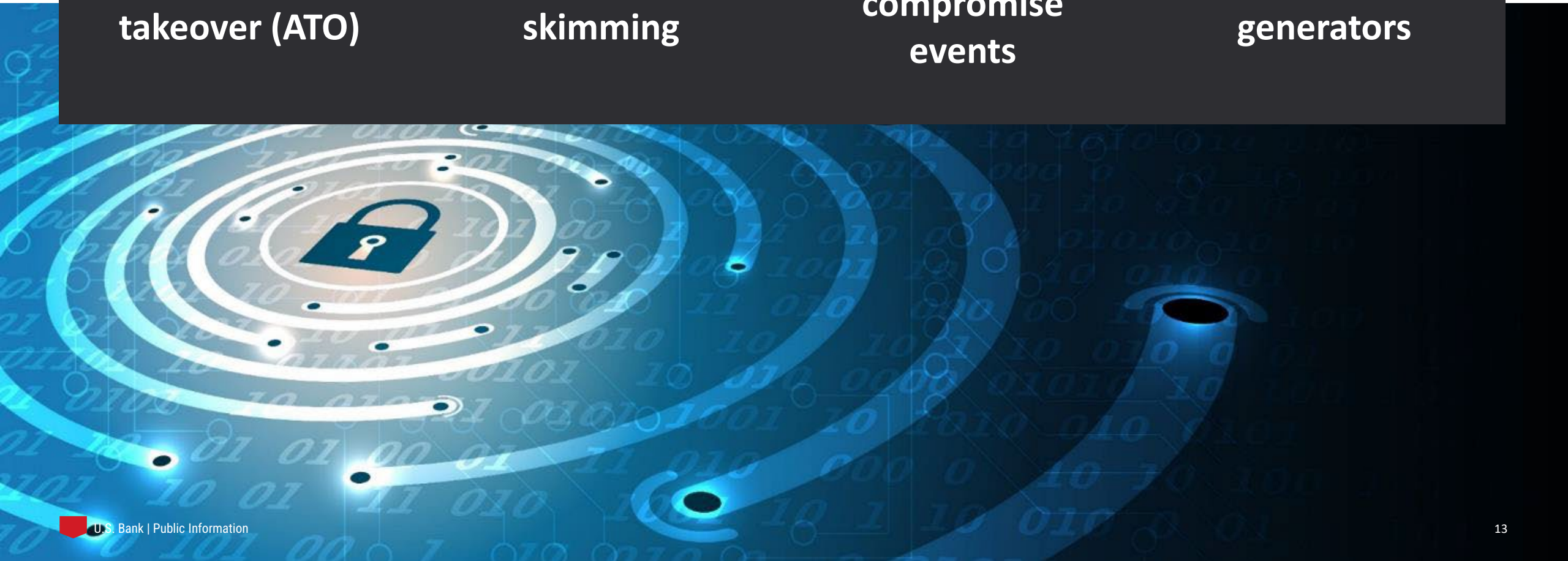
Stay ahead of other fraud trends

Account takeover (ATO)

Counterfeit/ skimming

Merchant compromise events

Account number generators

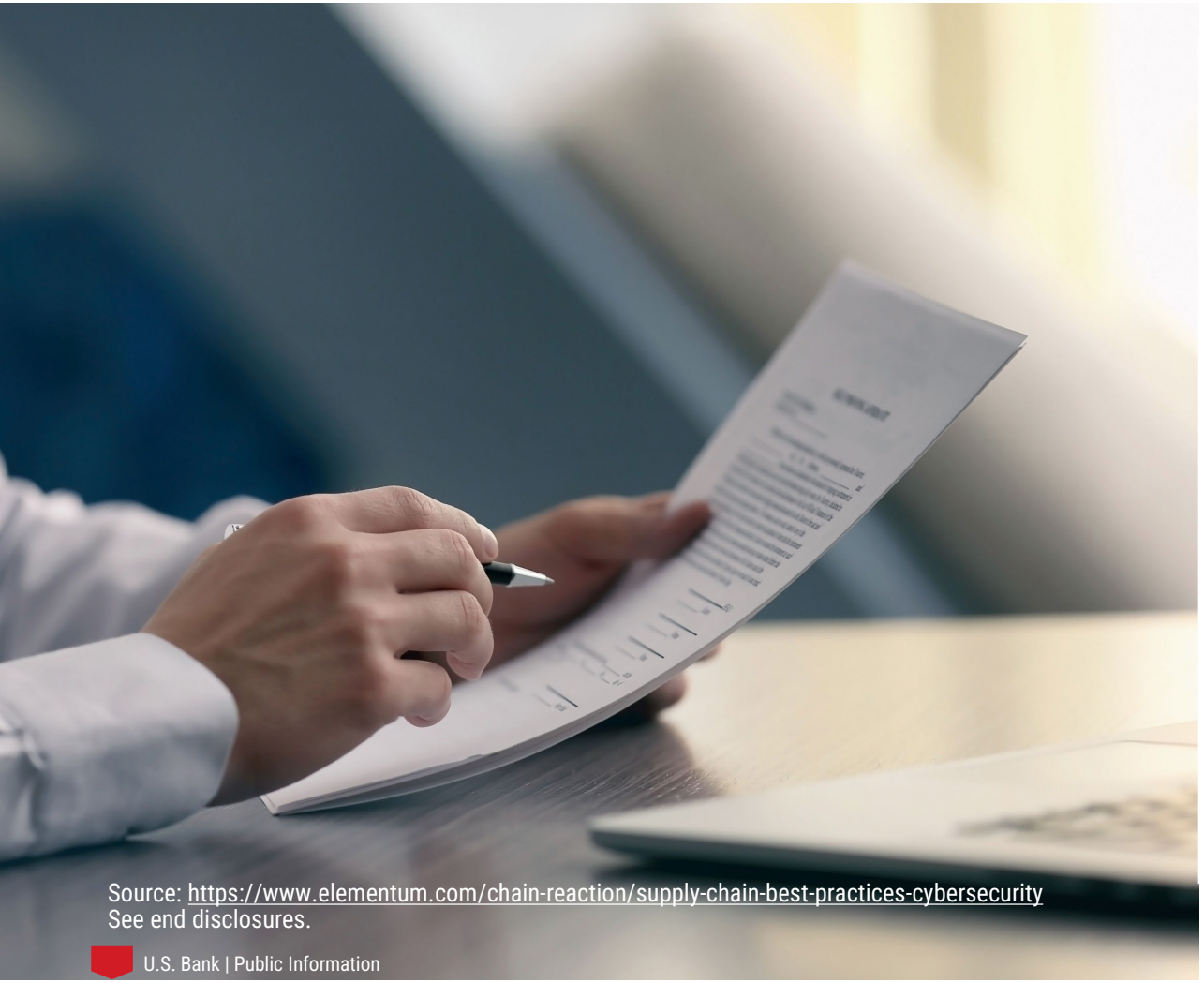


Strengthen your security protocols

- Implement dual control
- Trust but verify and reverify
- Communicate quickly
- Use strong authentication
- Create awareness
- Protect workstations
- Implement blocks and filters

Managing supply chain and third-party risk

You’re as strong as your weakest link; this includes your vendors



Source: https://www.elementum.com/chain-reaction/supply-chain-best-practices-cybersecurity
See end disclosures.

Contracts should address security and the handling of data.

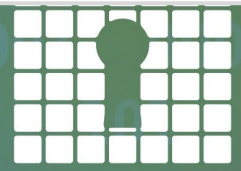
Control information privilege; employ need-to-know principle. What access is really needed?

Continuously monitor vendors and software providers’ security posture.

Know the critical suppliers – those that touch your systems, network or sensitive info.

Managing risk – access rights and controls

Ongoing controls	Quarterly management controls	Annual management controls
• Management approval of user access requests • Exception roles for transmitting confidential information and remote access • Immediate termination of access for terminated employees	• User access audit • Certification of direct reports exception roles • Access model certification	• Certification of access models • Annual certification of enterprise roles



See end disclosures.

2023 OACTFO Conference

Cybersecurity and risk

In the era of remote working

Potential threats related to remote work

Computing	Physical	Voice
• Business email compromise. • Phishing emails related to Centers for Disease Control, World Health Organization, etc. • **Personal email use for official business.** • Unsecure Wi-Fi networks.	• Leaving equipment outside employee's control. • Equipment not locked-down. • Untrustworthy person in home. • Printing of sensitive information.	• Teleconferencing software security vulnerabilities. • Zoombombing. • Personal assistant devices always listening. • Sensitive information discussed via third-party tools.

See end disclosures.

To avoid cyberattacks

Cybersecurity & Infrastructure Security Agency (CISA), the Federal Bureau of Investigations and National Security Agency encourage the cybersecurity community to adopt a heightened state of awareness and to conduct proactive threat hunting.

1

Be prepared.

Confirm reporting processes and minimize personnel gaps in IT/OT security coverage. Create, maintain, and exercise a cyber incident response plan, resilience plan, and continuity of operations plan so that critical functions and operations can be kept running if technology systems are disrupted or need to be taken offline.

2

Enhance your organization's cyber posture.

Follow best practices for identity and access management, protective controls and architecture, and vulnerability and configuration management.

3

Increase organizational vigilance.

Stay current on reporting on this threat. Subscribe to CISA's mailing list and feeds to receive notifications when CISA releases information about a security topic or threat.

Source: 2022 – Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.
See end disclosures.

Our remote work cyber risk resources

- Stop Ransomware
- Business email compromise: Recognize a scam
- Protect your business
- Report suspicious activity or fraud to your bank

See end disclosures.

Cybersecurity disclaimers

These websites, and the services provided, are under the exclusive control of the respective third-party provider. These links are provided as a courtesy and do not imply, suggest, or constitute any sponsorship, endorsement, or approval of any third party or any affiliation with any such third party. Further, we make no warranties or representations whatsoever with regard to any third-party website, merchandise, or service, and we are not responsible or liable to you for any damages, losses, or injuries of any kind arising out of your use of any third-party website.

This information has been obtained from sources believed to be reliable, but we cannot guarantee its accuracy or completeness.