



Risk & Compliance Solutions | Webinar

Cyber Landscape Threats

Navigating the evolving cyber environment

Proprietary and confidential. Do not distribute.



Today's session



Brianda Rojas-Levering

Senior Risk Consultant – Kentucky



Andrea McKay

Claims Manager
Beazley Insurance Services



Max Bradshaw

Cyber Services Manager
Beazley Insurance Services



→ | **What's on tap?**

Risks are evolving

Cybersecurity is one of the most dynamic risks for organizations to manage

Confidentiality

If the confidentiality of your data is breached; it has been stolen or copied.

Phishing attacks are a common method of breaching data's confidentiality or privacy.

Integrity

The integrity of your data refers to its accuracy and safety.

Perpetrators of a data integrity breach aim to alter, corrupt, or even completely destroy data or complete information systems.

Availability

Data availability is your ability to access it.

Ransomware and distributed denial-of-service (DDoS) attacks are two common methods of compromising data availability.



- Human Element
- Business email compromise/ fraudulent instruction
- Phishing
- Ransomware
- Third-party vendor incidents
- Litigation

On the radar

From a claims perspective, what would you consider to be in the top 3 most prevalent threats?

A woman with long, curly brown hair is looking down at a laptop screen. She is wearing an orange top. The background is a blurred office environment with a window showing greenery.

How do these cyber threats affect
small credit unions – if at all?

Susan in Wisconsin



The Human Element

How people are getting hooked



74% of breaches include the human element, such as errors, stolen credentials, and other forms of social engineering.

Source: 2024 Verizon Data Breach Investigations Report

Common human threats

- Poorly protected passwords
- Clicking on unsecure and damaging files and emails
- Unsure about their abilities to prevent an attack
- Lack knowledge about cybersecurity policies and practices for their organization
- Lack of awareness about the organization's process to report suspected cyber attacks even when their organization has a process in place
- Lack of ongoing education on cybersecurity risks and risk management strategies



Business Email Compromise & Fraudulent Instruction

Ease of providing instruction + the quickness of moving large sums of money

Business email compromise

\$2.9 billion adjusted loss for BEC crimes against businesses & consumers.

Source: IC3's 2023 Internet Crime Report, FBI

- A fraudster compromises an exec's email and then sends a well-crafted email to another member of the c-suite or employee with instructions to complete a transaction.
- The recipient complies with the email message and authorizes the payment or information release often without following appropriate follow-up protocols.
- The money or data is then wired to or shared with the fraudster as the instructions requested.

63% of organizations experienced some form of attempted or actual BEC in 2023.

Source: 2024 Payments Fraud and Control Survey Report, Association for Financial Professionals



Red flags: BEC

- Sense of urgency
- Requests typically come from a high-level executive
- Often coincide with being out-of-the-office
- Requests to keep transaction confidential and only communicate through email
- Often coincide with changes in direct deposit information or for payments to be made to a different account
- May impersonate a trusted supplier, vendor or partner
- Misspellings, poor grammar and emails sent outside of normal business hours

Less than 60% of organizations created written policies and procedures to safeguard against BEC.

Source: 2024 Payments Fraud and Control Survey Report,
Association for Financial Professionals



Human element

Which key strategies and/or technologies do you use to minimize the risk of human threats?

Social engineering fraud & phishing

How people are getting hooked

Primary types of phishing

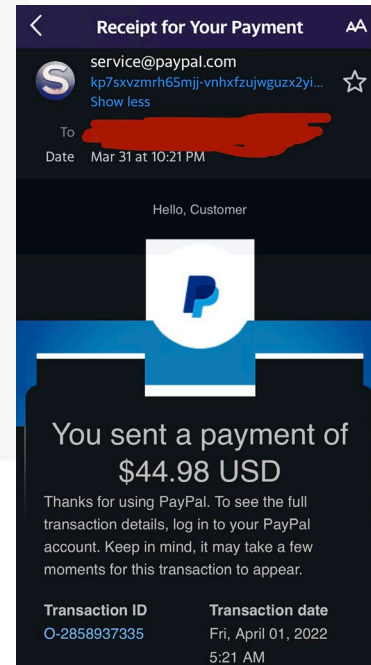
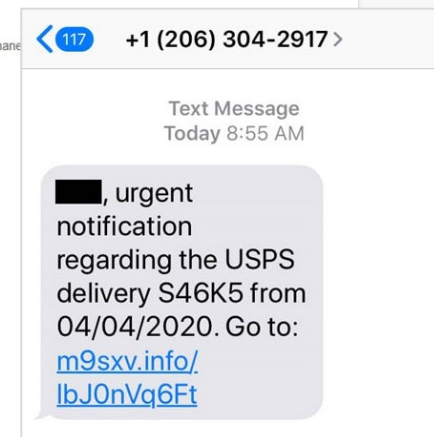
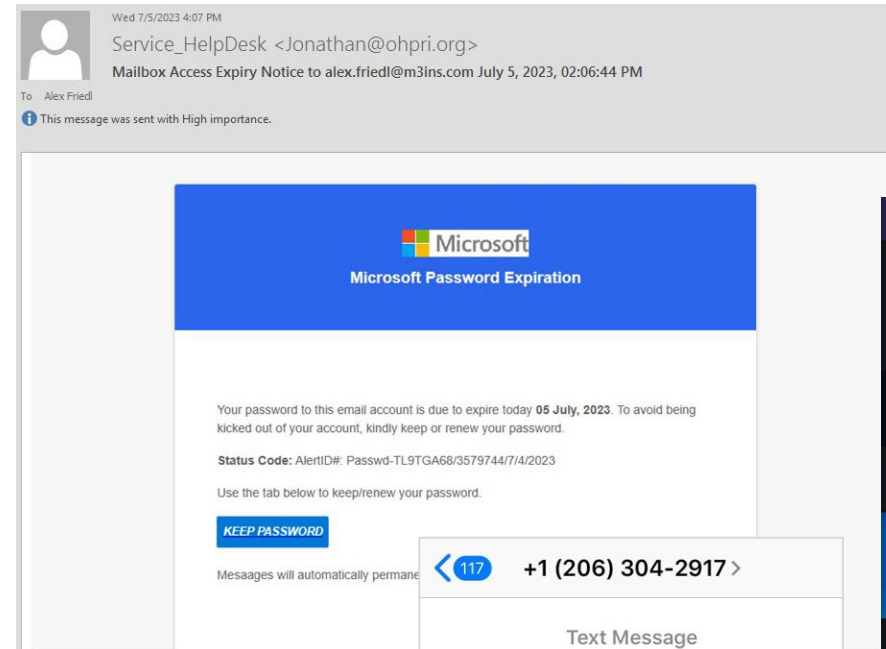
Phishing • SMiShing • Vishing

Share sensitive information

Trick the user to share sensitive information like login credentials (username/password) or account numbers that can be used to breach a system or account.

Download malware

Get the user to infect their own computer by downloading malware through an embedded link to a malicious or spoofed website or an attachment.





Intimidation tactics and urgent requests are common.

Key mitigation tips:

- Email filtering
- Employee education & training
- Phishing simulations

If you receive an attempt at social engineering fraud or a phishing email, you should delete it or use your phishing or credit union's established fraud reporting system immediately.

Notify your IT department, but do not open, respond, or provide information!

Ransomware

Attacks and payments have escalated in frequency, scope, and volume

Ransomware attacks

Six and seven-figure ransomware demands have become routine

Most identified infection points

- Phishing emails
- Corrupt attachments
- Weak remote desktop protocols (RDP)
- Unpatched systems
- Extensive reuse of passwords
- Lack of multi-factor authentication

Roughly one-third of all breaches involved ransomware or some other form of extortion technique.

Source: 2024 Verizon Data Breach Report

\$391K

Average ransom payment paid by ransomware impacted companies

77%

Of attacks threaten to leak exfiltrated data

Source: Ransomware Quarterly Report, Coveware, July 2024

Proactive prevention measures

- Keep all systems, software, and cloud locations patched and up-to-date
- Activate two-factor / multi-factor authentication on all systems
- Backup and test data regularly and verify the integrity
- Apply the principles of least privilege and network segmentation
- Vet and monitor third parties that have remote access to your network and other third-party connections
- Gain familiarity with FinCEN's Red Flag Indicators
- Provide regular social engineering and phishing training with employees



Are scams getting more sophisticated with AI?

Lindsey in Louisiana



Third-party relationships

While you can outsource the service; remember, you still own the responsibility

Third parties



Supply chain attacks make it easier for cyber attackers to circumvent security controls by creating avenues to sensitive resources through targets of third, fourth, and nth party vendors.

68%

Increase of data breaches involving third parties from 2023

Source: Verizon Data Breach Report, 2024

73%

Total reported incidents since 9/1/2023 involved compromises with a third-party

Source: NCUA, 2024



- Sound vendor due diligence
- Understand your vendors and how they protect your data
- Review your vendor's data security standards and strategies
- Consider putting contract provisions, security requirements and risk oversight in place to best manage organizational resources
- Know how your third-party vendors rely on their own set of subcontractors or fourth parties
- Formalize standards and expectations for security and compliance through SLAs



Governing third-parties

Compromising the right partner is a force multiplier for threat actors. Consider these vital steps for managing third-party relationships.

- Know your vendors – maintain an easily accessible list of all third-party vendors and what type of access they have to your credit union and member data
- Take necessary steps to understand your vendors' data security standards
- Know your vendors' cybersecurity strategies. If your third-party vendors are entrusted with your credit union's member data, their cybersecurity strategy is just as important as your own
- Set expectations for your vendor relationships. When making relationships with new third-party vendors, make cybersecurity a part of the vetting process and ongoing monitoring
- Understand your risk. Establish processes to evaluate and manage associated third-party risks before entering, during, and even after the vendor relationship ends
- Understand incident reporting - NCUA 72 Hour Rule and Vendor incidents

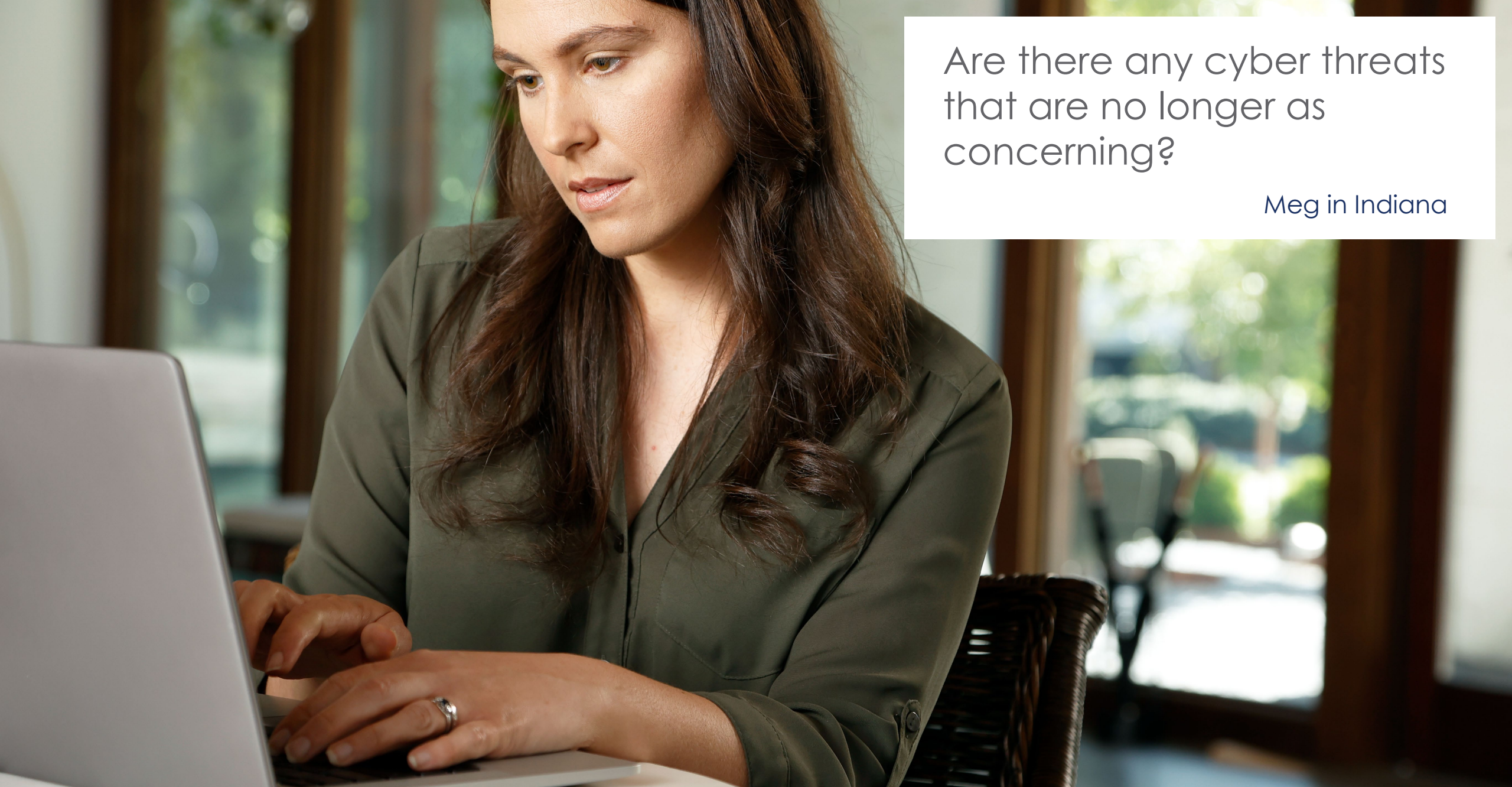


- With the increased focus on consumer data rights, more litigation is quickly becoming a significant risk to credit unions resulting from consumers who claim they have suffered damage as a result of a cybersecurity attack
- Uptick in Class Action lawsuits

Tips to minimize the litigation risk


- Practice good security hygiene
- Take proactive measures to protect data
- Report to cyber insurance carrier

Litigation landscape



Are there any cyber threats that are no longer as concerning?

Meg in Indiana



What are some of the common issues or mistakes you see within triage?

Key takeaways



Cybersecurity strategies continue to quickly evolve as do data security threats. Stay on top of next-generation vulnerabilities to minimize risk and be prepared to respond to potential loss of info and data.

- Commit to a thorough understanding of cyber threats – including those that are anticipated down the road
- Understand the risks and potential impact that your partners and vendors bring
- Prioritize and monitor cyber threats on an ongoing basis
- Strengthen your risk posture across the entire organization by delivering training, education, and instilling risk management knowledge & collaboration
- Promptly report incidents to your insurance carrier

How can AI be incorporated responsibly to identify cyber threats?

Dianna in Florida



Risk resources

Business Protection Resource Center www.trustage.com/bprc

- RISK Alerts – warning | watch | awareness
- Loss prevention library
- risk overviews, checklists & whitepapers
- Emerging risks outlook
- Live webinars, risk forums & office hours
- On-demand learning & interactive training modules

“Great information, excellent format. Presenters were engaging and knowledgeable in their respective fields.”

Executive Vice President - \$3B credit union

Risk resources

Beazley Breach Solutions www.BeazleyBreachSolutions.com

The screenshot displays the Beazley website's risk resources page. The header features the Beazley logo and navigation links for 'Prepare', 'Investigate', 'Respond', and 'Trends & Developments'. A secondary navigation bar includes 'USA', 'Services', 'Report an Incident', and a search function. The main content area is titled 'Start managing your cyber risks.' with a 'Get started now' button. Below this, a 'What's new' section highlights five articles:

- Uncovering supply chain security risks** (7 Jun): Learn how to minimize supplier cybersecurity risks, including risks from interconnected services like cloud vendors, and take actionable steps to protect your digital assets.
- 2024 Cyber risk predictions** (7 Jun): Our latest Cyber Services Snapshot discusses AI- and privacy-related litigation, website tracking technology claims, advances in cybercriminal techniques, and more.
- Implementing MFA for Microsoft 365** (8 Jun): Learn how to prepare for deployment and implement MFA for the Microsoft 365 environment.
- New SEC cybersecurity rules: Compliance and enforcement risk** (16 Nov): Learn what the new SEC reporting rules mean for public companies, how to comply, and what the enforcement risks are.
- Business continuity planning**: Preparing for possible interruption of your business operations is essential to being a resilient organization. Learn how to get started.
- Grr!tBreach Episode 4: Backups**: How good backups can help you recover from ransomware, and what challenges stand in the way.





Contact us

800.637.2676

- riskconsultant@trustage.com
- [Ask a risk manager interactive form](#)
- [Schedule a 1:1 risk consultation](#)
- [Report a risk or scam](#)



Thank you.

Contact

riskconsultant@trustage.com

800.637.2676

This presentation was created by the CUNA Mutual Group based on our experience in the credit union and insurance market. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value and implementing loss prevention techniques. No coverage is provided by this presentation/publication, nor does it replace any provisions of any insurance policy or bond.

TruStage™ is the marketing name for TruStage Financial Group, Inc., its subsidiaries and affiliates. TruStage Insurance Products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company. Cyber policies are underwritten by Beazley Insurance Group or other nonaffiliated admitted carriers.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy. Please read the actual policy for specific coverage, terms, conditions, and exclusions.