TWHC | Turner, Warren, Hwang & Conrad AC
Certified Public Accountants & Consultants

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA

NACUSAC Cybersecurity Training

Presented by Kian Moshirzadeh, CPA, CISA, CBA

NCUA Letter to CUs 24-CU-02
Subject: Cybersecurity

Course Topics

- Cybersecurity Overview
- Part 748 – Guidelines for Safeguarding Member Information
- Providing Recurring Training
- Approving Information Security Program
- Overseeing Operational Management
- Incident Response Planning & Resilience
- What You Can Do Personally

Cybersecurity Overview

- The frequency, speed and sophistication of cyberattacks have increased at an exponential rate.
- Foreign adversaries and cyber-fraudsters continue to target all critical infrastructure — including credit unions and other financial institutions.
- Since the NCUA's cyber incident notification rule, from September 1, 2023 through August 31, 2024, federally insured credit unions reported 1,072 cyber incidents.
- Seven out of ten of these cyber incident reports were related to the use or involvement of a third-party vendor.

Ransomware Attacks

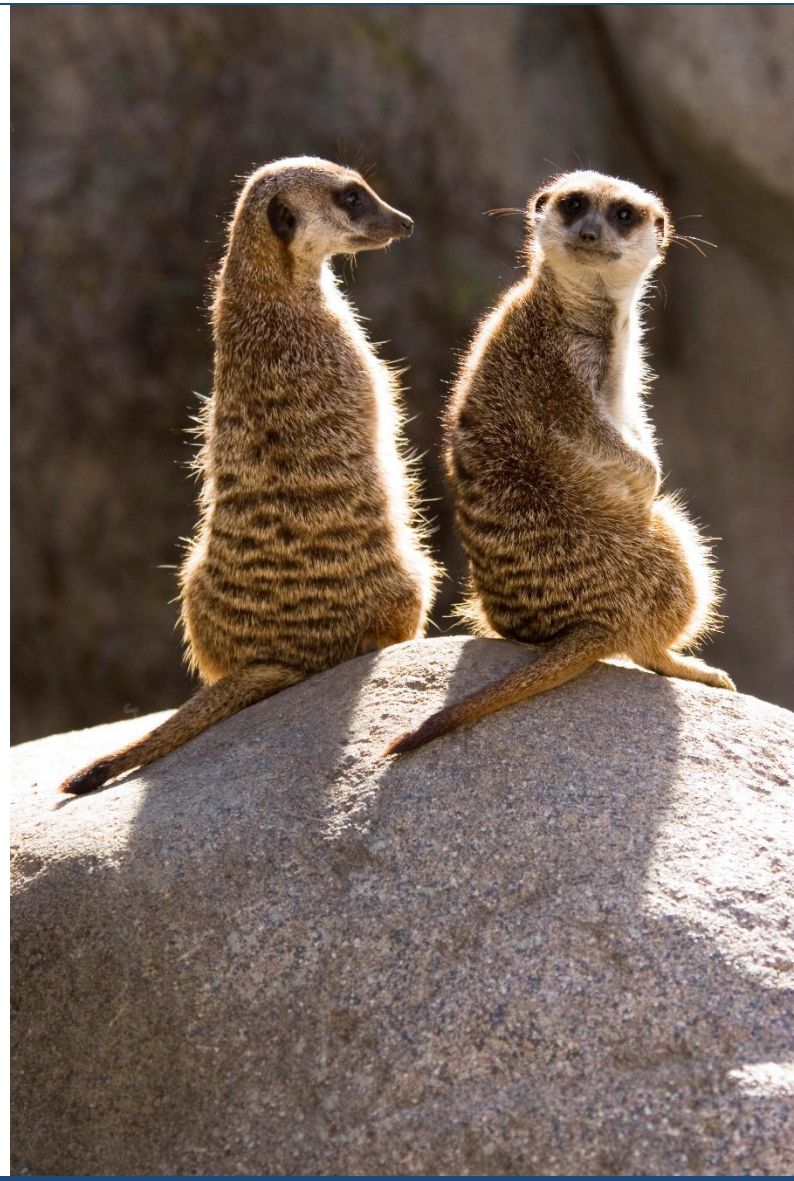
- A recent ransomware attack on a credit union has been attributed to “malvertising,” a relatively new cyberattack technique that injects malicious code within digital ads.
- For this type of attack to work, the user does not even have to physically click on a link for the system to become infected.
  - Instead, a simple internet search can result in malvertising that exploits the vulnerabilities in an internet browser.
- Credit union cybersecurity teams should focus on standardizing and securing web browsers and deploying ad blocking software to protect against this threat.

Cybersecurity Attacks

- The NCUA urges credit union boards of directors to prioritize cybersecurity as a top oversight and governance responsibility.
- Credit union board directors must ensure that a credit union's senior leadership is highly focused on managing cyber risks and that the credit union has the necessary resources to maintain an effective cybersecurity program that aligns with the products, services, and risk profile of the institution.
- This means making sure as a Board you provide the necessary budget to help management protect member information.

Key Areas

- The NCUA is recommending four key areas for boards of directors to focus on:
  - Providing Recurring Training
  - Approving Information Security Program
  - Overseeing Operational Management
  - Incident Response Planning and Resilience

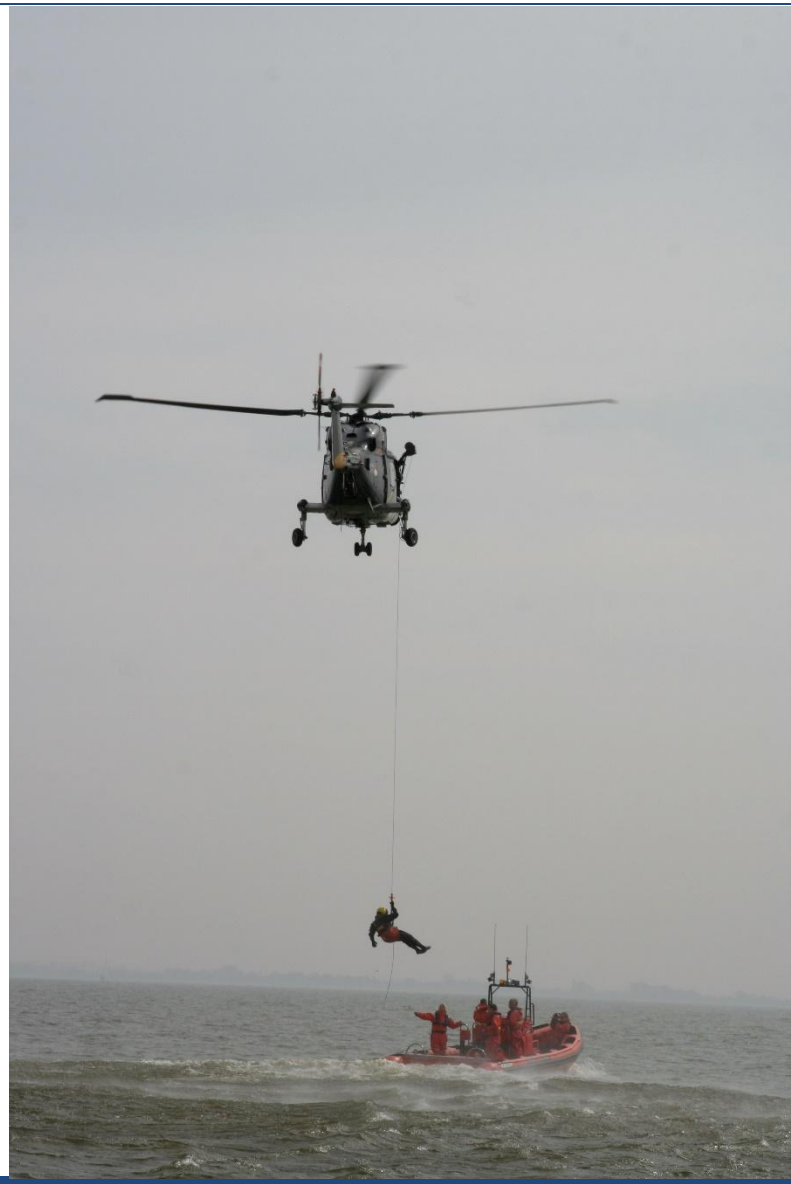


Providing Recurring Training

- The board should engage in ongoing education about current cybersecurity threats, trends, and best practices.
- The NCUA provides various resources to assist, including training webinars and written guidance, which can be found on the NCUA website.
- The board needs to stay aware of the specific cyber risks that pertain to the credit union's operations and the implications of these risks.
  - A subcommittee of the board can do this by routinely meeting to discuss results from IT Risk Assessments.
- Board members do not need to be technical experts, but they must know enough about cybersecurity to provide effective oversight and direction for the executive team and subject matter experts.
- The board should ensure the credit union's employees receive regular cybersecurity education to maintain high awareness and preparedness across the organization.
  - This education should emphasize the importance of a security-minded culture and adherence to important information security practices to mitigate the risk of cyber incidents.

Approving Information Security Program

- The board must approve a comprehensive information security program that meets the requirements of Part 748 of the NCUA's regulations, which includes:
  - Risk Assessments
  - Security Controls
  - Incident Response Plans
- The credit union board should review the program at least annually to ensure it adapts to the evolving threat landscape and incorporates lessons learned from past incidents.



Monitor Progress

Item #	Focus Areas for Board of Directors	Status	Verification
1	**Provide for Recurring Cybersecurity Training**	50%	The Board-approved Security Policy fulfills this area with respect to employee security awareness / cybersecurity training. The Board, however, does not receive ongoing Cybersecurity training. The Volunteer Education Policy will be updated to reflect this new recommendation from the NCUA and to ensure the Volunteers receive this training.
2	**Approve Information Security Program at Least Annually**	100%	Approval of the Security Policy, which includes the establishment of an Information Security Program, is conducted annually.

Overseeing Operational Management

The board is responsible for overseeing management of the credit union, focusing on the following cybersecurity areas:

- Third-Party Due Diligence
- Embedding Cybersecurity and Operational Resilience into the Organizational Culture
- Resources
- Vulnerability/Patch Management and Threat Intelligence
- Audit Function
- Reporting
- Protecting and Managing Backups
- Member Education

Overseeing Operational Management

- ***Third Party Due Diligence*** | The board should set clear expectations for management about the due diligence of third-party vendors with respect to information security. The credit union must ensure that contracts with third-party vendors include specific cybersecurity requirements, like timely notification to the credit union of any incidents, and clauses that protect credit union and member data.
- ***Embedding Cybersecurity and Operational Resilience into the Organizational Culture*** | The board and management should ensure that cybersecurity is a core value within the credit union, influencing decision-making at all levels.
- ***Resources*** | The board must provide management access to cybersecurity expertise and an adequate budget to implement and maintain a cybersecurity posture commensurate with the credit union's risk profile. The board should also encourage needed investment in cybersecurity technologies and tools to enhance the credit union's defenses.

Overseeing Operational Management

- ***Vulnerability/Patch Management and Threat Intelligence*** | The board must ensure that operational management places high emphasis on diligent vulnerability management, including timely software updates, patch management, and whitelisting and blacklisting URLs, websites, and software to mitigate risks. The credit union should use threat intelligence to stay informed about emerging threats and vulnerabilities that could impact the credit union. Government resources such as the Cybersecurity and Infrastructure Security Agency's cyber hygiene service for vulnerability management and the US Treasury's automated threat information feed are free to credit unions.

- ***Audit Function*** | Consistent with the size and risk profile of the credit union, the board should ensure management engages external parties with the requisite expertise to conduct audits of the cybersecurity program, to receive an objective assessment of program effectiveness.

- ***Reporting*** | The board should establish a framework for periodic reporting by management to the board on cybersecurity audits, incidents, and the effectiveness of the cybersecurity program. This reporting should include cybersecurity risk assessments, along with the identification of threats, vulnerabilities, and the effectiveness of controls. These reports should describe the overall status of the program. Reports should also outline material matters related to the program, including risk assessments, risk-management and control decisions, service provider arrangements, results of testing, and any recommendations for changes in the cybersecurity program.

Overseeing Operational Management

- ***Protecting and Managing Backup*** | In the face of increasing ransomware threats, credit unions must implement robust backup strategies to safeguard credit union and member data. The board should ensure management regularly backs up all critical data and that these backups are securely stored. Implementation of access controls will also prevent unauthorized access to backup data.

  In addition, the credit union needs clear, documented procedures for restoring data from backups in the event of a ransomware attack or data loss incident. This process should include identifying which data is critical for operations and prioritizing its restoration. Backup systems should be tested regularly to ensure that data can be restored quickly and effectively. Conducting routine drills will help identify any gaps in the backup process and ensure that staff are familiar with restoration procedures.

- ***Membership Education*** **|** The board should work with management to provide periodic information security education for members to promote sound cybersecurity practices, such as the use of multi-factor authentication and the importance of strong, frequently changed passwords.

Report Progress

Item #	Focus Areas for Board of Directors	Status	Verification
3	**Oversee Operational Management**		Fulfilled by the responses to 3.01-3.08 (with exception noted to 3.08
3.01	Third-Party Due Diligence	100%	This is fulfilled by our Vendor Management Policy.
3.02	Embedding Cybersecurity and Operational Resilience into the Organizational Culture	100%	The following items attest to this area: The Board-approved IT budget, which reflects consistent investments in Cybersecurity infrastructure and expertise, including an out-sourced virtual CISO; the Board-approved Security Policy, which places a heavy emphasis on information security awareness training; and a fully developed BCP Program, as required by Board-approved policy, which includes an annual DR and cybersecurity tabletop.
3.03	Resources	100%	This is fulfilled by the budget approval process. The Steering Committee has reviewed and recommended for Board approval IT budgets that include significant funds allocated to cybersecurity (software, hardware, and outside services).
3.04	Vulnerability/Patch Management and Threat Intelligence	100%	The following Board-approved policies fulfill this area: Security, Patch Management, Anti-phishing, and Anti-Malware.
3.05	Audit Function	100%	The Board-approved Security Policy fulfills this area, requiring reporting of audits to the Board through the SC via Internal Audit.

Report Progress

Item #	Focus Areas for Board of Directors	Status	Verification
3.06	Reporting	100%	The Board-approved Security Policy fulfills this area with regard to regular reporting, which the Incident Response Policy addresses time-sensitive reporting of security incidents.
3.07	Protecting and Managing Backups	100%	The Board-approved Security Policy fulfills this area.
3.08	Membership Education	50%	The Marketing Department fulfills this area. However, we must include this area in a Board-approved policy (Security Policy)

Incident Response Planning & Resilience

Incident Response Planning and Resilience

The board must, moreover, ensure that resilience plans allow the credit union to operate effectively during and after a cyber-attack. This planning may involve identifying alternative processes or systems that can be utilized during an outage. Consistent with statutory requirements, the NCUA's regulations require that a federally insured credit union that experiences a reportable cyber incident must report the incident to the NCUA as soon as possible and no later than 72 hours after the credit union reasonably believes it has experienced such an incident. This statutory requirement underscores the importance of having a well-defined incident response plan that enables prompt reporting and effective communication with regulatory bodies.

Effective resilience planning includes the following:

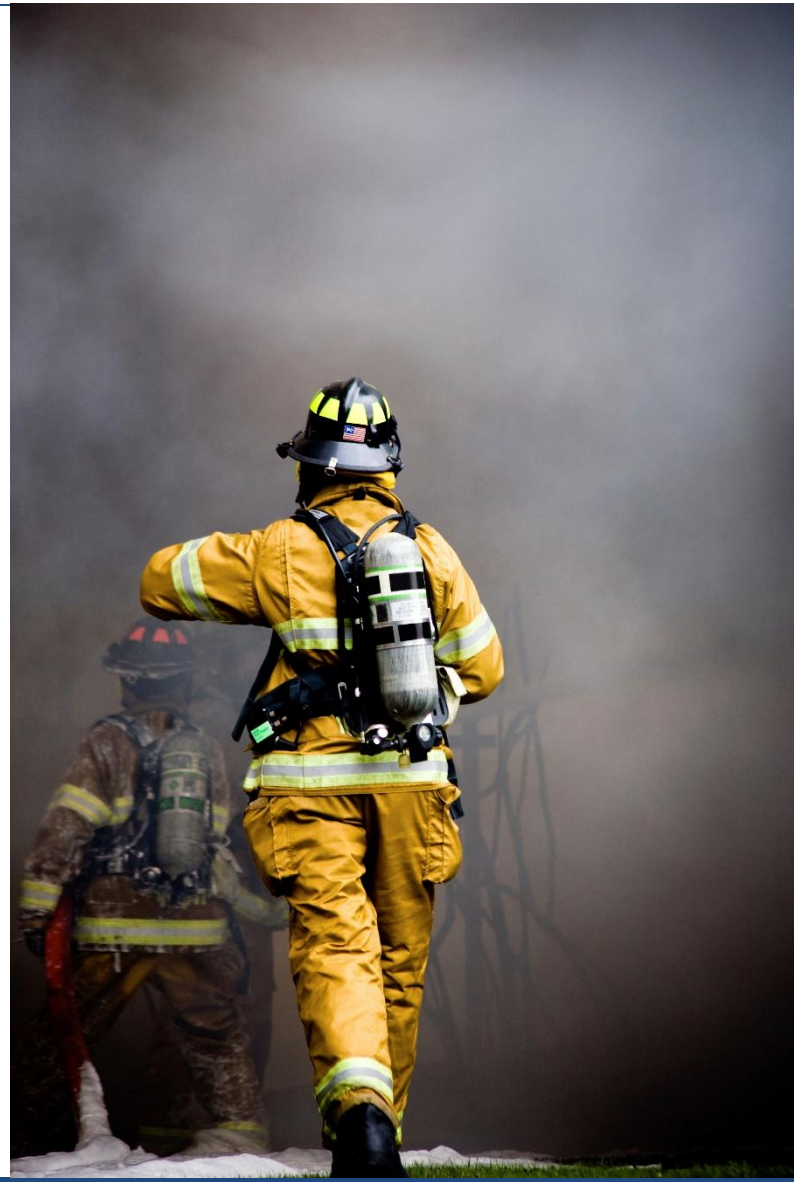
- ✓ ***Internal and External Communication*** | Establish a communication strategy for informing the board immediately following a security incident, ensuring transparency and timely decision-making. The communication strategy should also inform both internal stakeholders and external parties, including the members and regulators, in the event of a cyber incident. Clear communication can help manage expectations and maintain trust.
- ✓ ***Insurance Consideration*** | Evaluate cybersecurity insurance policies to ensure adequate coverage for potential incidents. This assessment includes understanding the scope of coverage and any exclusions that may apply.
- ✓ ***Incident Response Team*** | Identify and designate an incident response team that includes key personnel from various departments. This team should be prepared to take immediate action in the event of a cyber incident.
- ✓ ***Tabletop Exercises*** | Conduct regular tabletop exercises to simulate cyber incident scenarios. These exercises will help the credit union board and management practice response plans, identify areas for improvement, and ensure that all team members understand their roles during an incident.

Report Progress

Item #	Focus Areas for Board of Directors	Status	Verification
4	**Incident Response Planning and Resilience**	100%	The Board-approved Incident Response Policy fulfills this area. Testing results reported to ITSC annually.
4.01	Internal and External Communications	100%	The Board-approved Incident Response Policy fulfills this area.
4.02	Insurance Considerations	100%	Fulfilled annually by the CFO, VPs of Risk and IT to ensure adequate coverage; resented at the Board Meeting.
4.03	Incident Response Team	100%	The Board-approved Incident Response Policy fulfills this area.
4.04	Tabletop Exercises	100%	Conducted annually, led by Risk and IT, using our third-party vendor, and reported to the ITSC annually.

Conclusion

- By focusing on the key areas presented, the credit union's board of directors can significantly improve the credit union's cybersecurity posture and protect the interests of its members.
- Cybersecurity is not just an IT issue…
  - It must be a critical component of any credit union's overall governance and risk-management strategy.
  - A cyber incident can have far-reaching consequences, not only affecting the institution's financial stability, but also potentially impacting the entire financial services system while eroding member trust and damaging the credit union's reputation.
- By taking the proactive steps presented and prioritizing cybersecurity as a fundamental aspect of governance, the credit union's board of directors can effectively:
  - Safeguard the credit union and its members' assets
  - Maintain member trust
  - Ensure compliance with regulatory requirements
- We encourage you to consult the many available cybersecurity resources available on the NCUA's public website.



What can you do?

Cybersecurity Training

Where to Start

- Never give away credentials!
  - This is how most attacks happen and take shape: threat actors make a case to fool a person to give up their credentials
    - ✓ Email sent with a story to make it look like a legitimate request
    - ✓ SMS text or email with a link asking to click on it; once clicked, it will take you to a page that looks familiar and will ask you to input your user ID and password
    - ✓ Once credentials are entered and it does not work, you might enter a different user ID and password; all credentials entered will be collected
      - Attacker could potentially acquire both your banking and credit union network credentials
- Don’t use the same password for different accounts.
  - Most people only use one or two passwords associated with one or two user names across many platforms.
- Where possible, use a password vault and enable multi-factor authentication.

Cybersecurity Training

How Attackers Perform Reconnaissance

- LinkedIn and ZoomInfo
  - They see what positions you hold, who you report to and whether you are a board member. Then they start researching.
- Facebook and Instagram
  - They look at your profile and pictures.
  - They read comments on pictures to see who are your friends and relatives.
- BlockShopper and Zillow
  - They see when and how much you purchased your property for, and who else is on it.
  - They look at pictures of the home's interior if it was purchased in past five years.
    - Pictures may seem harmless, but can reveal your lifestyle and interests.
- Other websites
  - They find your age, relatives, where you are from, and financial history.

Information they glean is used to develop scenarios where it would make sense to ask you detailed questions and you would assume they know you or they are someone legitimately interacting with you.

In general, if anyone is asking for information:

- Verify who you are dealing with.
- Call them - do not rely on emails from them that might make sense.
  - Call on a number you have already, or you independently get.
- Do not rely on a number they give you.
  - If they say there is a problem with the normal number and you should contact them with a temporary number, that is a red flag.
- Do not give out or verify any of your information until you know the request is legitimate.
  - Once they have your information and start using it, the race is on to use the information to start their scam.