NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: **October 2024** **LETTER NO: 24-CU-02**

TO: **Federally Insured Credit Unions**

SUBJ: **Board of Director Engagement in Cybersecurity Oversight**

Dear Boards of Directors and Chief Executive Officers:

The frequency, speed, and sophistication of cyberattacks have increased at an exponential rate. Foreign adversaries and cyber-fraudsters continue to target all sectors of our nation's critical infrastructure — including credit unions and other financial institutions. From September 1, 2023, the effective date of the NCUA's cyber incident notification rule, 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.

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 doesn't 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.

Given the proliferation of sophisticated information security threats and the importance of safeguarding the assets and information of your members, the NCUA urges credit union boards of directors to prioritize cybersecurity as a top oversight and governance responsibility. Credit union board directors like you must ensure that a credit union's senior leadership is highly focused on managing cyber risks and that your credit union has the necessary resources to maintain an effective cybersecurity program that aligns with the products, services, and risk profile of your institution.

The following are four key areas your board of directors should focus on:

Provide for Recurring Training

Your board should engage in ongoing education about current cybersecurity threats, trends, and best practices. The NCUA provides various resources to assist, including training webinars, web-based learning resources, and written guidance. Your credit union board needs to stay aware of the specific cyber risks that pertain to your credit union's operations and the implications of these risks. Board members don't 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.

Furthermore, your 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.

Approve Information Security Program

Your 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, and incident response plans. Your 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.

Oversee Operational Management

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

- ***Third-Party Due Diligence***. Your 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.

- ***Embed Cybersecurity and Operational Resilience into the Organizational Culture***. Your board and management should ensure that cybersecurity is a core value within the credit union, influencing decision-making at all levels.
- ***Resources***. Your 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. Your board should also encourage needed investment in cybersecurity technologies and tools to enhance the credit union's defenses.
- ***Vulnerability/Patch Management and Threat Intelligence***. Your 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 U.S. Treasury's automated threat information feed are free to credit unions.[1]
- ***Audit Function***. Consistent with the size and risk profile of the credit union, your 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***. Your 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, including 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.
- ***Protecting and Managing Backups***. In the face of increasing ransomware threats, credit unions must implement robust backup strategies to safeguard credit union and member data. Your 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***. Your 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.

Incident Response Planning and Resilience

Your 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 that 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.[2]

Effective resilience planning includes the following:

- ***Internal and External Communication***. Establish a communication strategy for informing your 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 your members and regulators, in the event of a cyber incident. Clear communication can help manage expectations and maintain trust.
- ***Insurance Considerations***. 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 your credit union board and management practice response plans, identify areas for improvement, and ensure that all team members understand their roles during an incident.

Conclusion

By focusing on the key areas outlined above, your 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 your institution's financial stability but also potentially impacting the entire financial services system while eroding member trust and damaging your credit union's reputation.

By taking the proactive steps outlined above and prioritizing cybersecurity as a fundamental aspect of governance, your credit union's board of directors can effectively safeguard the credit union and its members' assets, maintain member trust, and ensure compliance with regulatory requirements. To that end, we encourage you to consult the many available cybersecurity resources available on the NCUA's public website not just during cybersecurity month in October but also year round.

Sincerely,

/s/

Todd M. Harper
Chairman

[1] *See* U.S. Treasury's Project Fortress Brochure (treasury.gov).

[2] *See* P.L. 117-103 available at PUBL103.PS (congress.gov).

Last modified on 11/27/24