Cybersecurity for the Board of Directors

2026 On-Demand Training and Certification

Presented by Steve Koinm, CISSP, CCSK, SAS-AP

PURE IT

Illinois Credit Union League

Steve Koinm
CISSP, CCSK, SAS-AP
CISO and Co-Founder
Steve.Koinm@pureitcuso.com

- Serves as the internal CISO for Pure IT Credit Union Services and as a virtual CISO or CIO to many clients while managing the vCISO practice for Pure IT
- Active in providing assessments and roadmaps for credit unions in People, Process, Technology, and Business Management
- An advisor to credit union Boards who need to provide a credible challenge to their technology teams and a regular speaker at security and credit union industry conferences throughout the country
- Advisory Board Member of the National Credit Union Information Sharing and Analysis Organization (NCU-ISAO).

Introduction

Why Board Cyber Training Matters

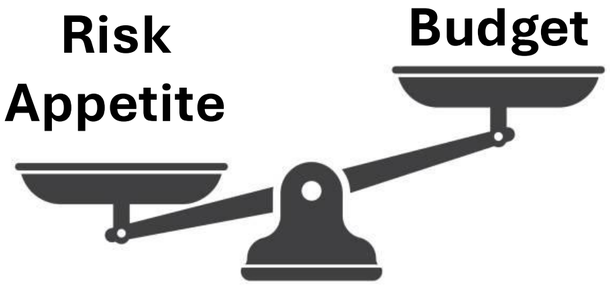
Cyber risk is business risk

- Cyber incidents directly impact member trust, operations, and financial stability
- Credit unions are increasingly targeted despite size
- Regulators explicitly expect board awareness and oversight, not delegation to IT alone

“By failing to prepare, you are preparing to fail.”

Ben Franklin

Cyber should be a TOP oversight priority



Cost of Cyber Breach in 2025

- $4.44MM worldwide
- 10.22MM in the US
- 60% of SMB fail after breach

PURE IT

Illinois Credit Union League

Key Areas of Focus

Board should provide the **Focus** and **Resources** to maintain an effective InfoSec Program

Training

Keep teams up to date.

InfoSec Plans

Written Information Security Plans

Operational Oversight

Board vs. IT vs. Management Roles

Incident Response

Clear processes during an incident

1. Training

- The Board must have baseline cyber training in all areas to provide a **credible challenge to management**
- You are responsible for **creating a culture of cyber awareness** in your organization
- Member education

Common Attack Vectors

Phishing

Malvertising

Weak credentials

Email Etiquette & Security Awareness Training

- Watch for: personal information requests, urgent requests, bad typos, odd URLs
- Use a tool like KnowBe4 to practice phishing awareness

Common Attack Vectors

Phishing

Malvertising

Weak credentials

Dynamic Cyber Protocols

- Keep software up to date (browsers, etc)
- Refresh training yearly, if not more
- Protecting and managing backups
- Stay aware of current threats with NCU-ISAO

Common Attack Vectors

Phishing

Malvertising

Weak credentials

Passwords and Access Management

- Length > complexity
- Use a password manager
- Enable multi-factor authentication
- Utilize the lowest level of access required

Artificial Intelligence

Understanding Risk vs. Reward

- AI can help your organization become more efficient and effective
- AI is also making threat vectors stronger and more realistic
  - Deepfakes

PURE IT

Illinois Credit Union League

2. Written InfoSec Plans

- Must meet **GLBA and Part 748**
- Must include **Risk Assessments, Security Controls, and Incident Response Programs**
- Must be reviewed and re-approved Annually to ensure it has adapted to **new threats** and **lessons learned**

3. Operational Oversight

- Third Party Due Diligence
- Embed Cybersecurity and Operational Resilience into the Organizational Culture
- Resources
- Vulnerability/Patch Management and Threat Intelligence
- Audit Function
- Reporting

Third Party - GLBA Guidelines

Due Diligence

- Evaluate vendor background, financial stability, reputation, and security controls
- Maintain an inventory of all third-party service providers
- Perform and document risk assessments before engagement

Contracts

- Require formal agreements for all vendors handling confidential data or critical services
- Clearly assign responsibility for protecting member and institution data
- Define security requirements, incident response roles, and enforcement/recourse
- Specify data return or destruction requirements at contract termination

Ongoing Monitoring

- Regularly update third-party risk assessments
- Review audits, assessments, and performance reports to validate security controls

3. Operational Oversight

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

4. Incident Response

- How can you operate during and after a cyber attack?
- Planning includes:
  - Internal and External Communication
  - Insurance Considerations
  - Incident Response Team
  - Tabletop Exercises

Thank you!

Next steps

- Complete your certification
- Reach out to info@pureitcuso.com with any questions for Steve
- Contact Illinois Credit Union League with any additional questions

Brought to you by

PURE IT

Illinois Credit Union League