

THE BUSINESS LEADERS SERIES

Cybersecurity for Business Leaders

CU EDITION

CYBER RISK, OVERSIGHT, AND MEMBER PROTECTION

A GOVERNANCE GUIDE FOR CREDIT UNION BOARDS AND EXECUTIVES

*Compliance is a floor,
not a ceiling.*

Govern to your actual risk. Let compliance follow.



THIS GUIDE · 2 OF 6 IN THE SERIES

J.W. WALKER · [JEREMYWALKER.US/RESOURCES](https://jeremywalker.us/resources)

Cybersecurity is no longer an IT problem. It is a governance responsibility. When a ransomware attack locks your core system or a vendor breach exposes member data, you don't face an IT failure. You face a credit union failure: regulatory scrutiny, legal liability, and the erosion of member trust. This guide is written to help you govern that risk in plain business terms, without needing to become a technical expert.

TWO PRINCIPLES THAT SHOULD GUIDE EVERYTHING

Before the domains, the controls, and the checklists, two ideas should shape how your board reads everything that follows. Get these two right and the rest becomes judgment. Get them wrong and no amount of tooling will save you.

Compliance is a floor, not a ceiling. Passing your NCUA examination means you cleared the minimum bar the regulator sets, not that your credit union is secure. A credit union with a spotless exam record can still be breached tomorrow. Compliance confirms baseline adequacy; it does not confirm safety. Govern to your actual risk, and let compliance follow as a byproduct, never the other way around.

Govern the risk you cannot delegate. The board does not manage firewalls or read scan results. But the board owns the decisions management cannot make alone: what risk the credit union will accept, whether findings are actually being resolved, whether the program is funded, and whether the reporting it receives is appropriate and honest. Those cannot be handed to IT. They are the substance of governance.

WHAT'S IN THIS GUIDE

1. Cybersecurity in the Boardroom	Why cyber risk is now a board responsibility, and what that means
2. The Threat Landscape	The attacks credit unions actually face today
3. AI and Emerging Threats	Deepfakes, AI fraud, and governing the AI your staff already uses
4. The Security Landscape	The core security domains in plain English
5. Identity Is the Control Plane	Why identity, not the firewall, is where the fight happens
6. Data Protection and Member Trust	Where member data lives and how to protect it
7. Vendor and Third-Party Risk	Why third-party exposure dominates reported incidents, and the CU-specific problem
8. Resilience, Backups, and Continuity	Recovering when, not if, something goes wrong
9. The Risk Management Process	A six-step framework the board can actually oversee
10. Testing, Audits, and Assessments	What each review tells you, and what it does not
11. Executive Metrics That Matter	A board dashboard that measures the right things
12. Questions to Ask Quarterly	A repeatable governance cadence
13. The First 90 Days	A checklist for new leaders and annual review
14. Your People Are Under Attack Too	Personal security for executives and board members

1. Why Cybersecurity Belongs in the Boardroom

In most organizations, cybersecurity was historically treated as an IT concern. That era is over.

When a ransomware attack locks your core banking system, branches cannot process transactions and members cannot access their accounts. When a vendor breach exposes member data, you face regulatory scrutiny, legal liability, and lasting damage to the trust that defines a credit union's relationship with its members. These are not IT problems. They are credit union problems.

A Note on Scope

This is a guide to cybersecurity and information security governance. Fraud is a related but distinct discipline, with its own controls, its own regulatory framework, and often its own team. The two intersect constantly: a compromised credential, a convincing deepfake, or an unpatched system is frequently the on-ramp to a fraud loss. This guide addresses those cyber weaknesses and the points where they open the door to fraud, but it does not attempt to cover fraud management, BSA/AML, or payments risk as disciplines in their own right. Those are major domains that deserve their own dedicated treatment.

Cybersecurity now touches every dimension of how a credit union operates:

- **Member trust.** A data breach or extended service disruption is a direct betrayal of the relationship members place in you. Trust, once damaged, is hard to rebuild.
- **Operational resilience.** Cyber incidents are now among the most likely causes of extended service outages. Business continuity and cybersecurity are the same conversation.
- **Regulatory posture.** Cybersecurity and information security remain significant safety-and-soundness concerns for regulators including NCUA, FFIEC, and state regulators. Reportable cyber incidents must be reported to NCUA within 72 hours. [4]
- **Financial exposure.** Ransomware payments, recovery costs, regulatory fines, legal fees, and forensic investigations represent material financial risk. Cyber insurance coverage depends on having adequate controls in place.
- **Vendor risk.** Your risk does not stop at your front door. It extends through every third-party vendor, cloud provider, and fintech partner with access to your systems or member data.

The Board's Role

The board's job is not to manage firewalls, select security tools, or interpret vulnerability scan results. Those responsibilities belong to management and technical staff. The board's job is to govern.

- Confirm that management has a funded, effective, and improving security program.
- Understand the credit union's material cyber risks in plain business terms.
- Ensure identified findings are tracked and resolved, not just reported.
- **Establish risk appetite and set the boundaries of acceptable risk.**
- Ask meaningful questions and expect straight, honest answers.
- Treat cyber risk with the same governance rigor applied to credit risk, liquidity risk, and compliance.

Governance Principle

A board that receives a clean audit report then moves on has not governed cybersecurity. Governance means ongoing oversight, informed funding decisions, and accountability for unresolved risks.

Does Your Board Need a Cyber-Literate Director?

Regulators and the broader financial sector have increasingly asked whether boards have the fluency to oversee cyber risk at all. You do not need every director to be technical, and you should be wary of any guide that tells you otherwise. But a board with no member who can engage credibly with a security report is a board that cannot tell the difference between reassurance and genuine progress.

There are three practical ways to close that gap. Recruit a director with security or technology risk experience. Provide structured cyber education to existing directors so the whole board can ask better questions. Or engage an independent advisor who reports to the board rather than to management, giving directors a second, unfiltered read on the program. Any of the three works. Governing blind does not.

2. The Threat Landscape Facing Credit Unions

Credit unions are not too small to be targeted. They hold member deposits, process payments, and maintain personal financial data. The following are some of the most significant categories of risk in the current environment.

Business Email Compromise (BEC)

BEC is one of the highest-dollar fraud categories facing financial institutions. Attackers compromise or impersonate an executive's email account and use it to authorize fraudulent wire transfers, redirect payroll, or manipulate vendors into changing payment instructions. These attacks frequently succeed not because of technical failures but because an employee followed an instruction without independent verification. No firewall stops a convincing email from a spoofed address.

Ransomware

Ransomware attacks encrypt your systems and data, rendering them unusable until a ransom is paid or backups are restored. Modern ransomware operators also steal data before encrypting it, threatening to publish sensitive member and employee information unless paid, a tactic called double extortion. Recovery, even with backups, can take days to weeks and is expensive. Ransomware attacks on core processors have cascaded into simultaneous service outages across dozens of credit unions at once.

Phishing and Spear Phishing

Phishing delivers malicious links or attachments via email, tricking employees into surrendering credentials or installing malware. Spear phishing is the targeted version, crafted for a named individual using researched details about their role and relationships. Finance teams, HR staff, executives, and system administrators are common targets. A single successful phishing attack is frequently the entry point for a larger breach.

Credential Theft and Account Takeover

Stolen usernames and passwords are traded widely on criminal markets. When employees reuse passwords or fail to use multi-factor authentication, attackers can access systems without exploiting any technical vulnerability. They simply log in. Member accounts face the same

threat: attackers test stolen credential lists against login portals at scale, then drain accounts, apply for loans, or open fraudulent products.

Supply Chain Compromise

When a core processor, managed service provider, or fintech partner is compromised, the impact extends to every credit union they serve. Credit unions without visibility into vendor security posture often do not learn about a vendor compromise until the damage is already spreading through their own systems.

Insider Risk

Not all risk comes from outside. Employees with privileged access can intentionally or accidentally expose data, modify records, or facilitate fraud. The risk is elevated during transitions: departing employees, disgruntled staff, or contractors with excessive access. Insider risk requires access controls, separation of duties, monitoring, and a formal offboarding process that revokes access immediately upon departure.

Cloud Misconfiguration

As credit unions move systems and data to cloud platforms, improperly configured storage, permissions, or access controls can expose member data to anyone on the internet. Many significant data exposures have resulted from misconfigured cloud settings, not external attacks.

Cyber-Enabled Payment Fraud

Payments fraud is its own discipline, but much of it now arrives through a cyber door. ACH origination, wire transfers, card processing, and mobile payment platforms are all targeted for direct financial gain, and the entry point is frequently a compromised credential, a spoofed email, or a socially engineered member service interaction rather than a flaw in the payment rail itself. This guide addresses that cyber on-ramp. The broader payments-fraud program, including transaction monitoring and recovery, sits alongside it as a distinct discipline.

Key Insight

Many successful breaches begin with a compromised credential, a clicked phishing link, or an exploited vendor rather than a technically sophisticated exploit. Human behavior and access management are where a large share of attacks start.

3. Artificial Intelligence and Emerging Threats

See also: *AI for Business Leaders*, the dedicated guide in this series, covers AI adoption, governance, and risk in depth.

Artificial intelligence is transforming cybersecurity from both sides. Defenders use AI to detect threats faster and process security signals at scale. Attackers use AI to conduct more convincing, more targeted, and more scalable attacks. Credit union leaders need to understand three dimensions: the threats AI enables against your organization, how AI is reshaping fraud and account takeover, and how to govern the AI tools your own staff is already using.

AI-Enabled Threats Against Your Credit Union

Deepfake voice and video. AI voice-cloning tools can replicate a person's voice from as little as a few seconds of recorded audio, often sourced from a voicemail, a public video, or a social media clip. Attackers use cloned voices to impersonate executives, board members, or members themselves. Fraud scenarios now include a cloned "CFO" calling an employee to authorize an urgent wire transfer after hours, a "board chair" calling the CEO during a sensitive decision window, and fake member voices used to bypass telephone authentication at member service centers. Deepfake video is advancing at similar speed and is already appearing in fraud attempts against financial institutions. [8]

Board Member Awareness

Your voice may be a target. Recordings from public board meetings, recorded calls, or social media can be harvested to create convincing audio impersonations. Any executive or board member with a public profile should treat unusual verbal requests for action or money as suspect until independently verified.

AI-generated phishing at scale. Traditional phishing emails were often identifiable by poor grammar or awkward phrasing. AI-generated phishing can eliminate many of those signals, producing grammatically perfect, contextually aware messages that reference a recipient's actual job title, colleagues, recent work, or organization-specific terminology scraped from public sources. What once required a skilled operator hours to craft can now be produced in seconds across thousands of targets at once. The human filters trained on “bad grammar” and “suspicious links” are increasingly insufficient on their own.

AI-assisted attack tooling. Attackers are beginning to use AI to speed up parts of their work, from writing convincing lures to helping analyze targets. The practical takeaway for leaders is not a specific technique but a direction: the time between when a weakness becomes known and when it is used may continue to shrink, which raises the value of testing and patching on a disciplined cadence.

AI in Fraud and Account Takeover

Synthetic identity fraud. AI enables the creation of synthetic identities at scale, fabricated persons assembled from real identity fragments combined with generated information, used to open accounts, build artificial credit history, and ultimately commit bust-out fraud. Detection is difficult because no real individual is being directly impersonated, and the pattern can look like a legitimate member for months before the bust-out occurs.

Cyber-enabled account takeover. Automated credential-stuffing and related techniques let attackers test large volumes of stolen credentials against login portals and work around some traditional controls. Where a compromised credential leads to a drained account or a fraudulent loan, a cyber weakness has become a fraud loss. The defense is the same one that matters everywhere else in this guide: strong identity controls, MFA, and monitoring.

Social engineering of member services staff. Member service employees field calls daily requesting account changes, password resets, and transfers. AI voice impersonation means the caller may not be who they claim to be, even if they sound exactly right. Staff must be trained on verification procedures that do not rely on voice recognition or caller familiarity alone. Secure callbacks to registered numbers, step-up authentication, and other independently verified controls are stronger than knowledge-based questions alone.

Governing Your Own AI Tool Usage

Many credit union employees are already using AI tools in their daily work, whether formally sanctioned or not. Staff use consumer AI assistants to draft member communications, summarize documents, analyze loan data, and answer operational questions. The governance question is not whether AI is being used. It is whether its use is visible, controlled, and consistent with member privacy obligations.

Shadow AI and data exposure. When employees enter member data, internal policies, account details, or financial records into public AI tools, that information may be used to train external models, retained by the provider, or exposed in ways that violate member privacy, regulatory requirements, or contractual obligations. This risk is largely invisible without a policy framework defining what may and may not be used with AI systems.

A governance framework for AI tool usage should address:

- Which AI tools are approved for use, and by which roles.
- What categories of sensitive data may be used only in specifically approved AI environments, and what data or uses are prohibited entirely.
- How AI-generated content is reviewed before use in member-facing communications, regulatory filings, or credit decisions.
- How AI vendors are subject to third-party risk review, the same as any other technology vendor.
- Who maintains the approved tool list and reviews new tools before use.
- How employees report accidental disclosure of restricted data through AI tools.

Regulatory expectations for AI. NCUA's current position is that its existing regulations are technology-neutral: AI is supervised through the frameworks that already apply, and AI vendors remain subject to the same due diligence and third-party risk management as any other vendor. [6] In practice that means existing expectations around fair lending, vendor due diligence, and whatever model-risk discipline you already apply can extend to AI tools used in underwriting, member communication, or operational decisions. The governing principle for leaders is simple: a decision a credit union cannot explain is a decision it cannot defend to an examiner or a member, so AI use in consequential decisions must be documented and auditable.

Leadership Question

Ask your technology and compliance teams: What AI tools are employees using today? What member data may have passed through those systems? Do we have a policy that governs this, and have employees been trained on it?

4. The Security Landscape in Plain English

A mature security program covers many domains. Leaders do not need to understand how each technology works. They need to understand what each domain protects and what questions to ask about it.

Identity and Access	Controls who can log in to what, with what permissions. Weak identity controls are involved in a large share of breaches. The most important domain.
Endpoint Security	Protection on laptops, desktops, servers, and mobile devices. Unmanaged or unprotected devices are a primary attack surface.
Email Security	Filtering of malicious messages before they reach employees. Phishing remains one of the most common attack delivery methods.
Network Security	Firewalls, segmentation, and traffic monitoring. Limits how far an attacker can move once inside.
Cloud Security	Securing data and systems hosted in cloud platforms. Configuration errors are a leading cause of cloud incidents.
Data Protection	Encryption, classification, and access controls on sensitive data. Protects member information at rest and in transit.
Application Security	Security in the software and web applications the credit union runs. Poorly secured apps are common targets.
Backup and Recovery	The ability to restore systems and data after an incident. Backups are only valuable if tested and confirmed to work.
Vendor Security	Oversight of third-party security posture. Your risk extends to every vendor with access to your systems or data.

Monitoring and Detection	The capability to detect threats in near-real time. Undetected threats cause far more damage over time.
Incident Response	A defined process for identifying, containing, investigating, and recovering from an incident.
Governance and Policy	The policies, training, risk management, and accountability that tie all other domains together.

5. Identity Is the Control Plane

Many leaders still think of the firewall as the center of security. In modern environments, identity is often where the fight starts and ends.

When an attacker steals valid credentials and uses them to log in, there is no attack for a firewall to block. The attacker looks exactly like a legitimate user. Defense shifts to strong identity controls, behavioral monitoring, and meaningful access limitations.

Multi-Factor Authentication (MFA)

Multi-factor authentication requires something you know (a password) plus something you have (a phone or hardware token) or something you are (a biometric). Even if an attacker has a stolen password, MFA makes that password alone insufficient in most cases. For a credit union, MFA should be required for all administrative and privileged accounts, all remote access, email and collaboration platforms, core banking and financial systems, any system containing member data, and vendor and third-party access accounts.

Board Question

What percentage of accounts require MFA today, especially privileged accounts and remote access? What is the target coverage and the timeline to reach it?

Privileged Access Management

Privileged accounts, those with administrative rights or the ability to modify security configurations, are the highest-value targets for attackers. A compromised admin account can disable security controls, delete backups, and move freely across the network. Leaders should confirm that privileged accounts are inventoried and reviewed on a schedule, that

administrative access uses separate accounts from day-to-day use, that access is granted on a least-privilege basis, that privileged sessions are logged, and that access is revoked immediately when employees change roles or leave.

Password Management and Account Lifecycle

Password reuse is one of the most exploitable behaviors in any organization. When employees use the same password across work and personal accounts, a breach of any one becomes a credential the attacker can test against all the others. Password managers and long, unique passwords meaningfully reduce this risk. Equally important is lifecycle management: without a formal offboarding process, former employees retain access long after they leave. Regular access reviews should verify that every account is tied to an active, authorized person with a current business need.

6. Data Protection and Member Trust

Member data is the most sensitive asset a credit union holds. Social Security numbers, account numbers, transaction histories, loan applications, and personal financial information are exactly what identity thieves and fraudsters want. Leaders need to understand where that data lives, who can access it, how it is protected, and what happens if it is exposed.

Where Member Data Lives

Member data rarely lives in one place. It may reside in the core banking system, loan origination platform, card processor, email archives, document management systems, scanned records, cloud storage, backups, and on employee devices. Vendors you share data with may hold copies you no longer track. A meaningful data inventory answers: What sensitive data do we have? Where does it live? Who has access? How long do we retain it? How is it destroyed when no longer needed?

Encryption, Retention, and Destruction

Encryption converts data into an unreadable format without the appropriate key, and should apply both at rest and in transit across databases, file shares, email, mobile devices, and backups. Equally important, data you no longer need is still a liability: retaining data beyond its required period increases the scope of any breach without providing value. A formal retention

schedule defines how long each record type is kept and how it is securely destroyed, including paper records, hard drives, archived backups, and decommissioned systems.

Regulatory Requirements and Member Notification

Credit unions are subject to overlapping data protection requirements. For federally insured credit unions, the Gramm-Leach-Bliley Act is enforced through NCUA's member-information safeguarding requirements under Part 748, which call for a documented information security program appropriate to the credit union's size and risk. [5] State privacy laws add obligations that vary by the location of your members. When member data is exposed, notification obligations trigger at multiple levels: NCUA requires notification of a reportable cyber incident within 72 hours, and state breach notification laws impose their own member-notice timelines. [4] Leaders should know what the notification process looks like, who authorizes it, and what legal counsel is engaged before an incident occurs.

Data Governance Question

Do we have a current data inventory? Do we know where member PII lives across all systems and vendors? When did we last review our retention practices and confirm that data destruction is actually occurring on schedule?

7. Vendor and Third-Party Risk

No credit union is an island. Core processors, cloud providers, fintech partners, managed service providers, payment processors, and dozens of other third parties have access to your systems, your data, or both. When any of them experience a security incident, you may experience one too.

Why Vendor Risk Is the Central Story

This is not a peripheral concern. NCUA reported that, of the 1,072 cyber incidents federally insured credit unions filed in the first year of the notification rule (September 2023 through August 2024), seven out of ten were related to the use or involvement of a third-party vendor. [1] The concentration risk is real and concrete: a single 2023 ransomware attack on a shared service provider disrupted 60 small credit unions at once. [2] One vendor failure can ripple across many institutions in a single event.

There is a structural wrinkle unique to the credit union world that boards should understand plainly. Unlike the banking regulators, NCUA does not have direct supervisory authority over third-party service providers. It cannot examine your core processor, your cloud provider, or your fintech partners directly. Both the Government Accountability Office and the Financial Stability Oversight Council have urged Congress to restore that authority, but until they do, credit unions operate without a regulatory backstop on the vendor side. [2][3] In practical terms, NCUA is not independently examining your critical vendors for you. Your credit union remains responsible for risk-based due diligence, contractual protections, ongoing monitoring, and contingency planning. That oversight is yours to perform, and examiners increasingly expect to see that you are performing it with current information, not last year's questionnaire.

The 72-Hour Rule Extends to Your Vendors

NCUA's cyber incident notification rule requires you to report a reportable incident within 72 hours. For an incident at a third party, that clock starts at the sooner of two moments: when the vendor notifies you, or when you otherwise form a reasonable belief that the compromise or disruption occurred. A vendor that sits on the news for a week does not automatically put you out of compliance, but it does leave you dangerously little room, and it can mean the reasonable-belief clock was already running while you waited. That is why vendor contracts must obligate prompt notification: not as a nicety, but so that you can reliably meet your own deadline. Notification timelines in critical vendor contracts are now a regulatory necessity. [4]

Components of a Mature Vendor Risk Program

- **Vendor inventory.** A current list of all vendors with system or data access, classified by criticality. An inventory you cannot maintain is not a real inventory.
- **Due diligence.** Security assessments before onboarding, including review of SOC 2 reports, penetration test results, security questionnaires, and insurance coverage.
- **Contractual controls.** Security requirements, incident notification timelines, audit rights, and breach response obligations must be present in contracts, not assumed.
- **Ongoing monitoring.** Periodic reviews at intervals appropriate to vendor risk, not just at contract renewal. A high-risk vendor reviewed only every three years is not meaningfully monitored.

- **Concentration risk.** When multiple critical functions depend on a single vendor or technology stack, that concentration warrants additional oversight and contingency planning. This is acute in the credit union space, where a small number of core processors serve much of the industry.

Vendor Risk Reality

An attacker who compromises your managed service provider may gain administrative access to your environment without ever attacking you directly. Because NCUA cannot directly examine your providers, responsibility for effective due diligence and ongoing oversight remains with the credit union. Vendor oversight is not optional. It is a fundamental component of your security program.

8. Resilience, Backups, and Continuity

Resilience is the ability to withstand disruption and recover with acceptable speed. In a cybersecurity context, it means being able to detect an incident, contain the damage, restore systems and data, and resume member service within a timeframe that members and regulators can accept. A common failure mode is not the absence of backups. It is the presence of backups that have never been tested and fail when they are needed most.

Backup Fundamentals

- **Recovery Point Objective (RPO).** How much data can the credit union afford to lose? If the last backup ran 24 hours ago, a ransomware attack today means 24 hours of transactions are potentially gone. Backup frequency should be designed to meet a defined RPO.
- **Recovery Time Objective (RTO).** How long can operations be disrupted before the impact becomes unacceptable to members and regulators? The RTO drives investment in redundancy, failover, and recovery infrastructure.
- **Offline and immutable backups.** Backups stored only on the same network as primary systems can be encrypted or deleted by ransomware. Critical backup strategies should include offline, segregated, or immutable copies that an attacker with ordinary production access cannot modify or delete.

- **Backup testing.** A backup that has never been tested has not been proven to work. Restoration tests must run on a regular schedule, cover all critical systems, and be reported to leadership. A failed restoration test for a critical system should be treated as a critical finding.

Business Continuity and Incident Decision-Making

Business continuity planning defines how the credit union operates when primary systems are unavailable: which member services must be maintained and at what minimum level, manual procedures for teller transactions and payments when core systems are down, communication protocols for members and regulators, and clear decision authority. When an incident occurs, decisions must be made quickly and with incomplete information. Who has authority to disconnect systems? Who authorizes a forensic firm? Who notifies NCUA? Who communicates to members? These questions must be answered before an incident, not during one. Incident response plans should be reviewed annually, and contact information and escalation paths verified whenever they change.

The Ransom Payment Decision

One incident decision deserves its own attention because it carries legal exposure the board must understand in advance: whether to pay a ransom. This is not simply a financial or operational choice. Paying certain sanctioned threat actors can itself be a violation of federal law, and regulators have made clear that a payment made without appropriate diligence can create liability on top of the incident. [7] The decision should never be made in the heat of an attack by whoever happens to be available. No ransom decision should be made without legal counsel and sanctions screening; both are non-negotiable before any payment, not optional steps.

Before an incident, the board should confirm who holds authority to authorize or refuse a payment, that legal counsel and sanctions screening are part of any payment decision, and that procedures exist for appropriate engagement with law enforcement.

Board Question

When were our backups last tested? Were all critical systems included? What were the results? How long would it actually take to restore full operations after a ransomware event, and who has authority over the decisions we would face in the first 24 hours?

9. The Risk Management Process

Cybersecurity risk does not manage itself. It must be identified, evaluated, prioritized, and actively addressed through a structured process that is visible to leadership and reported to the board. The following six steps are the essential framework every credit union should operate.

Step 1: Define Risk Appetite

Risk appetite is the amount and type of risk leadership is willing to accept in pursuit of the credit union's mission. It is a governance decision made by the board and senior leadership, not a technical determination made by IT. For cybersecurity, risk appetite statements set the boundaries within which management operates, for example: the credit union will not accept unencrypted member PII on any production system; will not operate core banking without tested, offline backups meeting a defined RTO; and will not onboard a vendor with privileged access that has not completed a security review within the past 12 months. Without a stated appetite, there is no consistent basis for prioritizing investment or knowing what requires board escalation. It should be reviewed and formally approved at least annually.

Governance Connection

Risk appetite translates the board's values into operational guidance. When management accepts a risk or defers a control, that decision should trace back to a documented risk appetite position, not informal judgment.

Step 2: Identify Critical Systems and Assets

Not all systems are equal. Before risk can be meaningfully assessed, the credit union must identify what matters most: the systems, data, and processes whose failure or compromise would cause the greatest harm. Core banking systems, payment systems, member data repositories, identity and authentication systems, network infrastructure, backup systems, and critical vendor connections form the backbone of that inventory. It is the foundation for everything that follows, and risk assessments, continuity plans, and security investment should all flow from a clear understanding of what the credit union cannot afford to lose.

Step 3: Assess the Risks

Risk assessment evaluates the likelihood and potential impact of threats against each critical asset, producing a prioritized view of where the greatest risk exists. A meaningful assessment considers the threat sources that could cause harm, the vulnerabilities they could exploit, the likelihood of the threat being realized given current controls, and the operational, financial, regulatory, and member-trust impact if it were. Risk assessments should be kept current, revisited as part of the annual information-security program review, and updated after significant changes: new systems, new critical vendors, major technology transitions, or material incidents.

Step 4: Maintain a Risk Register

A risk register is a living document recording identified risks, their current ratings, assigned ownership, planned treatments, and resolution status. It is the operational artifact that connects assessment findings to active management. Each entry should capture a plain-language description, a likelihood and impact rating, a named risk owner, a treatment plan, a current status with target dates, and the residual risk remaining after controls are applied.

Governance Use

The risk register is one of the most important documents a board should review regularly. It shows not just what risks exist, but whether management is actively addressing them, who owns them, and whether residual risk is within the board-approved appetite.

Step 5: Treat the Risks

For each risk, management selects a treatment. Mitigate: implement controls that reduce likelihood or impact, the path for most high-priority cyber risks. Transfer: shift financial impact through insurance or contract, though cyber insurance requires specific controls and does not cover all losses. Accept: formally decide not to invest further, typically when mitigation cost exceeds expected loss, with the acceptance documented, owned, and revisited. Avoid: eliminate the activity or asset creating the risk entirely.

Step 6: Monitor and Report to the Board

Risk management is not an annual event. Threats emerge, vendors change, systems are added and retired, and staff turn over. The board should receive a regular cyber risk update covering

the status of the highest-rated risks, any new risks identified, progress on active mitigation with items at risk of missing targets, a summary of incidents and near-misses, and any risks where the board-approved acceptance posture should be reconsidered.

Risk Appetite vs. Risk Reality

One of the most important governance questions is whether current residual risks are within the board-approved appetite. If open risks exceed the stated appetite, that gap should trigger escalation for additional mitigation, funding, or formal acceptance at the level authorized by the credit union’s governance framework.

10. Testing, Audits, and Assessments

Credit unions are subject to a range of security reviews. Understanding what each one is, and what it is not, prevents leaders from mistaking compliance activity for security assurance.

IT Controls Audit	Evaluates controls against a defined scope and set of criteria. May include testing of technical controls, but it is not adversarial testing against a live attacker.
Risk Assessment	Identifies and prioritizes major cyber risks by likelihood and impact. The output is a prioritization, not a certification.
Vulnerability Scan	An automated check for known technical weaknesses: missing patches, misconfigurations, known flaws. Produces a list of potential issues; does not validate or exploit them.
Vulnerability Assessment	Takes scan output further with human validation, context, and prioritization by severity and business impact. Separates real risk from scanner noise. Still stops short of exploitation.
Penetration Test	Simulates a real attacker attempting to breach systems. Demonstrates what an attack could achieve, within a defined scope and timeframe.
Social Engineering Test	Tests human susceptibility to phishing, pretexting, and vishing. Reveals training and process gaps.
Architecture Review	Evaluates whether the overall system design creates unnecessary risk. Particularly useful before major changes.

Configuration Review	Checks whether systems are configured against a prescriptive security benchmark such as the CIS Benchmarks. Distinct from a vulnerability scan and more rigorous.
Tabletop Exercise	A discussion-based simulation of an incident. Tests whether decision-making, communication, and escalation work in practice.
Compliance Examination	NCUA or state review of minimum regulatory standards. Meeting exam standards is a floor, not a ceiling.

Critical Limits Every Leader Should Understand

- **A clean audit does not prove security.** An audit evaluates controls against a defined scope and criteria. Even a thorough one is not the same as adversarial testing: passing it means you met the criteria examined, not that your defenses would hold against a determined attacker probing for the gaps the audit did not look at.
- **A vulnerability scan is not a penetration test.** A scan identifies known vulnerabilities. A penetration test actively attempts to exploit them. Very different levels of assurance.
- **A penetration test does not equal a mature program.** Surviving a scoped simulation means you passed that simulation, not that the broader environment is secure.
- **A tabletop exercise does not prove recovery readiness.** Unless the action items it surfaces are completed and validated, it identifies gaps without closing them.
- **Meeting exam standards is the minimum, not the goal.** Regulatory compliance confirms baseline adequacy. A credit union with an excellent exam record can still be successfully breached.

Testing Principle

Testing is only valuable if findings are acted on. Ask how many findings from the most recent penetration test or risk assessment remain unresolved, and why. The age of open findings is often more telling than the findings themselves.

11. Executive Metrics That Matter

Security metrics for the board should be meaningful, actionable, and honest. The following measures give a practical view of security posture without requiring technical expertise to interpret. If every metric trends green every quarter, ask what is being measured.

MFA Coverage (%)	What percentage of accounts require multi-factor authentication, especially privileged accounts? One of the highest-impact controls against credential-based attacks.
Privileged Account Review	When were privileged accounts last inventoried and reviewed? Are all tied to current, authorized individuals?
Critical Patch Compliance (%)	What percentage of systems have critical patches applied within the required window? Unpatched flaws are among the most exploited vectors.
Open High-Risk Findings	How many findings from recent assessments remain unresolved, and how long have they been open? Age matters as much as count.
Vendor Review Completion (%)	What percentage of critical vendors have been reviewed within the required cycle?
Backup Test Results	When were backups last tested across all critical systems? What were the results? Any failures?
Phishing Susceptibility (%)	What percentage of employees click simulated phishing tests? Is the rate improving, and which groups are most susceptible?
Security Incident Trend	How many incidents occurred this period? Is the count rising? What types are appearing?
Endpoint Protection (%)	What percentage of managed devices have endpoint security installed, updated, and active?
Training Completion (%)	What percentage of employees completed required annual security awareness training?
Time to Remediate	Average days between identification of a critical finding and its confirmed resolution.

Reporting Integrity

Honest security reporting shows a mix of progress and problems. A board dashboard with nothing in the red or yellow columns every quarter is a signal that the reporting framework needs to be challenged, not that the credit union has no security challenges.

12. Questions Every Board Should Ask Quarterly

These questions create a repeatable governance cadence. They do not require technical expertise to ask, but the answers reveal whether the security program is functioning, improving, and honestly reported. Ask them consistently, and expect the answers to change.

1. What are our top cyber risks right now, and what is the status of efforts to address them?
2. What changed in our environment this quarter? New systems, new vendors, significant configuration changes, or staff changes in security-sensitive roles?
3. Where are we currently accepting risk, and is that acceptance still appropriate given what we know today?
4. What findings from our last assessment, audit, or penetration test remain unresolved? What is preventing resolution?
5. When were our backups last tested? Were all critical systems included? What were the results?
6. What is the status of our critical vendor reviews? Are any high-risk vendors overdue?
7. Are privileged accounts controlled? When were they last reviewed and reduced to the minimum necessary access?
8. What would cause the greatest harm to members if it failed or was compromised today?
9. What security improvements need funding, leadership authority, or executive decision-making to move forward?
10. Have we had any security incidents, near-misses, or threat intelligence updates the board should understand?
11. What AI tools are employees using, and are member data or sensitive records being handled appropriately within them?

Asking Better Questions

Security briefings that consist entirely of status updates create a false sense of progress. Boards that ask what is not going well, what is overdue, and what management is worried about get more honest and more useful reporting.

13. The First 90 Days: A Leader Checklist

For new executives or board members, and as an annual baseline review for all leaders, the following confirms that foundational oversight is in place and the credit union's security program is visible at the governance level.

Risk and Assessments

- Confirm a current risk assessment exists. Review the top findings and their status.
- Review all open findings from recent audits, assessments, and penetration tests, and how long each has been open.
- Confirm each open finding has a named owner, a resolution plan, and a target date.
- Review the risk register and confirm it is actively maintained and reported to leadership.

Identity and Access

- Validate that MFA is enabled for all administrative, remote access, and cloud platform accounts.
- Confirm privileged accounts have been reviewed within the past 90 days.
- Ask when the last access review was conducted, particularly for staff who changed roles or departed.
- Confirm a formal onboarding and offboarding process exists for system access.

Resilience and Backups

- Confirm backups exist for all critical systems and are stored offline or in immutable storage.
- Ask when backups were last tested, what was included, and what the results showed.
- Review the business continuity and incident response plans. Confirm they are current, tested, and understood.
- Confirm the NCUA 72-hour incident notification procedure is documented and the responsible individuals know it.

Vendors

- Review the vendor inventory. Confirm it is current and covers all vendors with system or data access.
- Identify any critical vendors overdue for a security review and ask why.

- Confirm contracts with critical vendors include security requirements, breach notification timelines that let you meet the 72-hour rule, and audit rights.
- Ask whether any critical service relies on a single vendor without a documented contingency.

Governance and Insurance

- Confirm the board receives a meaningful cyber risk report at least quarterly.
- Review cyber insurance coverage. Confirm limits, exclusions, and required controls are understood and met.
- Schedule a tabletop exercise within 90 days if one has not occurred in the past 12 months.
- Confirm legal counsel is identified for cyber incident response before an incident occurs, and that the ransom-payment decision authority is defined.

AI and Emerging Technology

- Ask whether a formal AI usage policy exists and whether employees have been trained on it.
- Confirm vendor-provided AI tools have been reviewed under the third-party risk program.
- Ensure executive and board-level awareness of deepfake voice and video risks, and that verification procedures exist for unusual financial requests.

14. Your People Are Under Attack Too

See also: *Personal Cybersecurity for Business Leaders*, the dedicated guide in this series, covers this in full and is built to share with staff, boards, and families.

Attackers do not only target systems. They target employees, executives, board members, finance staff, and their families. A compromised personal email account can be used to launch attacks against the credit union. A board member who falls for a deepfake voice scam can inadvertently authorize a fraudulent transaction. Personal security is now part of organizational resilience. The following is recommended for every executive, board member, and their household.

Protect Your Identity

- Freeze your credit with all three major bureaus (Equifax, Experian, TransUnion) and with ChexSystems. A freeze is free, can be temporarily lifted, and prevents new accounts from being opened in your name.
- Monitor your credit reports through AnnualCreditReport.com for accounts or inquiries you do not recognize.
- Set fraud and transaction alerts on all personal bank, investment, and credit card accounts.

Secure Your Accounts and Devices

- Enable MFA on every personal account, including ones that seem low value; attackers use them to pivot to higher-value targets.
- Use a password manager for strong, unique passwords, and never reuse them across work and personal use.
- Secure your personal email first. It is the master key to resetting almost every other account.
- Keep devices patched and enable full-disk encryption and remote wipe. For sensitive work away from home, prefer your own cellular connection or personal hotspot over unfamiliar Wi-Fi. A patched device using encrypted connections is what actually keeps you safe on an untrusted network; use a VPN where your organization requires one, but do not treat it as a substitute for the basics.

Guard Against SIM Swapping

SIM swapping is a fraud technique where an attacker convinces your mobile carrier to transfer your phone number to a SIM they control, giving them your text-based authentication codes. Add a port-out PIN or account passcode with your carrier, be alert to unexpected loss of cell service, and move critical two-factor authentication off SMS onto an authenticator app or hardware token where possible.

Be Skeptical of Unusual Requests

- Verify any unusual financial or authorization request through a separate, independently confirmed channel. Do not use the phone number or email the request came from.
- Remember that voice can be convincingly cloned from a small amount of audio. Urgent calls from executives or board members requesting money or sensitive information should always be verified through a second channel.

- Talk to family about scams, particularly voice impersonation and scams that target older relatives.

Reduce Your Digital Footprint

- Review your public social media presence. Details about your role, relationships, travel, and routines fuel targeted social engineering.
- Be aware that people-search sites and data brokers aggregate significant personal information; opt-out services can reduce this over time.
- Consider what is publicly visible on LinkedIn, association websites, and credit union materials. Attackers research targets before they make contact.

Leadership Reality

Executives and board members are high-value targets. Personal digital hygiene is also organizational security. The time you invest in protecting yourself is time invested in protecting the credit union and its members.

Closing: Security Is an Operating Discipline

Cybersecurity is not a product you purchase, a project you complete, or an audit you pass once a year. It is an operating discipline, practiced continuously, improved over time, and governed with the same rigor you apply to credit risk, liquidity management, and member service.

The credit unions that weather incidents best are not the ones with the most sophisticated tools or the largest IT departments. They are the ones with clear governance, honest reporting, tested plans, documented risk appetite, accountable ownership, and leadership that takes the subject seriously before something goes wrong.

Strong cybersecurity governance does not require every board member to become a technical expert. It requires asking the right questions, demanding honest answers, ensuring findings get resolved, requiring that risk is owned and tracked, and treating security investment as the operational necessity it has become.

The threat environment will keep evolving. AI-enabled attacks, more sophisticated fraud, and vendor compromise events will continue to affect financial institutions. A credit union's response is not to chase every trend or acquire every tool. It is to build the governance structures, recovery capabilities, and repeatable habits that make the organization resilient to whatever comes next.

A closing reminder on scope: the ground this guide covers is cybersecurity and information security governance. Fraud, BSA/AML, and payments risk are their own disciplines, closely connected to what is here but broader than it. Strong cyber governance closes many of the doors that fraud walks through, but it does not replace a dedicated fraud program. Treat them as partners, not substitutes.

Your members trust you with their financial lives. Security is how you protect that trust.

Sources and References

The regulatory facts and statistics in this guide are drawn from the following primary sources. Regulatory guidance evolves, so leaders should confirm current requirements with their own counsel and with NCUA before relying on any specific point for a compliance decision.

[1] NCUA, “Board of Director Engagement in Cybersecurity Oversight” (Letter to Credit Unions, October 2024). Reports 1,072 cyber incidents from September 1, 2023 through August 31, 2024, with seven out of ten related to the use or involvement of a third-party vendor.

[2] NCUA, Cybersecurity and Credit Union System Resilience Annual Report to Congress (June 2024). Source for the November 26, 2023 ransomware attack on a shared service provider that affected 60 credit unions, and for NCUA’s stated lack of vendor examination authority.

[3] U.S. Government Accountability Office, “Artificial Intelligence: Use and Oversight in Financial Services” (GAO-25-107197), and Financial Stability Oversight Council annual reports. Both recommend that Congress grant NCUA authority to examine third-party technology service providers.

[4] NCUA Cyber Incident Notification Requirements, 12 CFR Part 748.1(c), effective September 1, 2023 (NCUA Letter 23-CU-07, as updated by Letter 25-CU-02 in January 2025). Requires reporting a reportable cyber incident within 72 hours of forming a reasonable belief that it occurred; for a third-party incident, the clock runs from the sooner of vendor notification or that reasonable belief.

[5] Gramm-Leach-Bliley Act, Section 501(b), and NCUA 12 CFR §748.0, which establish mandatory information-security program requirements for federally insured credit unions; Appendix A provides the related Guidelines for Safeguarding Member Information.

[6] NCUA, Artificial Intelligence resource page and Credit Union AI Resource Center. States that NCUA has not issued AI-specific rules and that existing, technology-neutral regulations apply to AI use, with AI vendors subject to existing third-party due diligence expectations.

[7] U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. Warns that making or facilitating ransom payments to sanctioned actors can carry federal sanctions exposure.

[8] FinCEN, “Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions” (November 2024). Describes increased suspicious activity involving deepfake

media, including the use of synthetic audio and video to circumvent identity-verification and authentication controls.

About the Author

J.W. Walker has spent his career in information security across commercial and government environments. He has sat in the tester's chair, built a company from the ground up through exit, and serves as CTO of an information security firm. Today he advises executives and boards on technology strategy, security governance, and how to govern cyber risk without turning it into an IT-only conversation.

If your board wants an independent, unfiltered read on its security program, that is the work he does. Start at jeremywalker.us/cyber-advisory. More guides at jeremywalker.us/resources.

The Business Leaders Series

Plain-language guides for the decision-maker, not the technician. Each one takes a subject that is usually buried in jargon and makes it something a leader can actually use. If this guide was useful, the others are written the same way.

Penetration Testing for Business Leaders

What to test, what to ask, and how to turn findings into action.

Cybersecurity for Business Leaders: CU Edition *(you are reading this one)*

Cyber risk, oversight, and member protection, written for the board.

Cybersecurity for Business Leaders: SMB Edition

Cyber risk, protection, and practical steps for owners. Written with Ideal Technologys.

AI for Business Leaders

Getting real value from AI without getting burned by it.

The Virtual CISO for Business Leaders

What you are really buying when you hire fractional security leadership.

Personal Cybersecurity for Business Leaders

Protecting your identity, money, devices, family, and digital life. Built to share with your team and family.

Find the complete series at **jeremywalker.us/resources**

Last reviewed: August 2026. Regulatory positions and standards evolve; confirm specific requirements with counsel or your regulator before relying on them.