Blumira

White Paper

Credit Union Cybersecurity & Compliance

Discover how to align cybersecurity strategies with the core values of credit unions: service, community, and member financial benefits.

The Credit Union Difference

There's a reason more than 139 million Americans trust credit unions. They see the benefits every day—member-first service, community focus, and value returned through better rates and lower fees. The credit union difference shapes everything from technology deployment to branch planning—even cybersecurity and compliance strategies. Blumira understands credit unions.

Members First

Service is fundamental to credit union DNA. Financial institutions have long embraced technology to enhance member service, streamline operations, and stay competitive. For credit unions, digital transformation isn't merely about shifting transactions to more efficient channels where the consumer does all the work. It's about creating an engaging experience that provides easy account and product access any time, day or night.

$18.28M
average annual cost of cybercrime experienced by U.S. financial services companies according to Accenture.

Focus on Community

From the beginning, when credit unions were the only way many consumers could access financial services, credit unions have been providing vital services to the community. High levels of regulatory scrutiny can be frustrating, but it's a reflection of the role credit unions play as critical infrastructure—in a category with hospitals, transportation, and the power grid.

The first order of business, then, is keeping services up and running. Sadly, this is a real concern as criminals are successfully targeting smaller financial institutions with ransomware attacks that can take systems offline. Without a comprehensive cybersecurity strategy in place, trust built over decades can be shaken in days.

Returning Value to Members

Credit unions have a well-deserved reputation for lower fees and more attractive rates compared to banks. Member-ownership allows you to give back to members instead of paying shareholders. This value ethos also drives credit unions to budget wisely in order to use "profits" to add member convenience. With an efficient cybersecurity detection and response platform like Blumira, IT teams don't need to hire additional security experts or pricey consultants. Instead, you can focus resources on developing the next generation of products and services that help the credit union grow and attract younger members.

Perception or reality?

In their comparison of credit unions versus banks, Bankrate.com writes, "Some larger credit unions have advanced technology, but smaller credit unions might not."

With companies like Blumira building technology specifically for small–to–mid-sized organizations, this perception is quickly becoming antiquated.

Credit Union Cybersecurity

To support a members-first service commitment, your cybersecurity strategy needs to be both invisible and visible at the same time. Threat detection and response technology works behind the scenes to safeguard valuable assets and information. Visible, easy to understand access controls provide reassurance that security is your top priority. A cybersecurity strategy built around members will also align well with what regulators are looking for during their exams.

Solutions for Cybersecurity and Compliance Challenges

Grappling with 21st century cybersecurity challenges and the corresponding regulatory scrutiny can be enough to make an IT person question their career choices. The satisfaction of doing this work on behalf of credit union member-owners, though, gives it higher-level meaning. Blumira supports credit union IT teams with automated threat detection and response that helps fulfill your mission of protecting critical financial infrastructure—keeping member accounts and the organization safe and sound.

Here's how credit union IT teams use Blumira to solve cybersecurity and compliance challenges:

Keep Up with an Evolving Threat Landscape

Cyber criminals are always looking for new ways to exploit your systems—they're not going to let up. And they're embracing new technologies like AI as enthusiastically as everyone else. Yet remarkably, tried–and–true efforts to get employees and members to "click this link" continue to be depressingly effective as well.

Ransomware and data theft are increasingly prevalent, especially in small–and mid-sized organizations that criminals consider more vulnerable. That means cybersecurity must take a comprehensive, ever-vigilant approach.

An evolving cyber protection strategy is best accomplished with a flexible, cloud-based solution that scales with you:

- Blumira threat detection can be deployed throughout your environment, with a long list of integrations.
- Cybersecurity experts at Blumira are engaged in continuous threat hunting in order to update the platform and tune detections.
- Most Blumira subscriptions include 24/7 support to assist with threat analysis and mitigation.

Streamline Compliance Response

A recent change by the National Credit Union Administration (NCUA) defined a 72–hour window for cyber incident reporting. This has increased the urgency of federally regulated credit unions to have processes for accurate threat detection, immediate notification, and reporting. However, the 72–hour rule is just the latest in the high level of interest NCUA has for cybersecurity.

Security continues to have a prominent role in NCUA exams. Along with evaluating management, internal expertise, and the credit union's board of directors on their management of information systems and technology-related risks, the NCUA wants to confirm that internal information systems, technology controls, and oversight are sufficient to safeguard member information.

Protecting members is all part of being a credit union. Blumira makes that job easier with:

- Faster detection, so intruders have less time to explore your environment, and you can meet 72–hour requirements
- Unlimited activity log retention available for threat analysis and incident recovery.

Support Hard Working IT Teams

Already stressful IT jobs take on even more significance when members' money and critical data are at stake. Budget realities make it difficult to hire enough of the right people to monitor systems 24/7. And cybersecurity isn't your only priority. You simply can't set aside upgrades and new product development in favor of full-time threat monitoring.

IT personnel are more engaged and efficient when they have user-friendly tools to support them. Most Blumira users spend only 15 minutes a day on the platform. Blumira makes it easy to stay secure with:

- Automated detection and threat blocking so an intrusion is isolated while your team has time to investigate.
- Prioritized alerts that make it clear what level of response is required so that IT team members aren't wasting time on false alarms.
- Playbooks that walk users through action steps for every alert.
- Easy setup. You can be up and running quickly without hiring outside consultants to make it work.

Develop Solid Cybersecurity Plans

A comprehensive cybersecurity plan is the first step in protecting members and the credit union. It's also integral to demonstrating compliance when NCUA examiners are on the way. We can help you determine how the Blumira platform fits into your cybersecurity plans. Blumira customers rely on National Institute of Standards (NIST) and Center for Internet Security (CIS) frameworks to guide their planning. You can learn more about these frameworks here.

- The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is organized around a framework of core, profiles, and implementation tiers. The core consists of five detailed pillars that can be used as a planning guide and checklist.
- The CIS has developed a set of controls broken down into specific safeguards. Implementation Groups (IGs) help you prioritize CIS controls and safeguards based on the size and needs of your organization.
- NCUA recommends self-assessment by credit unions to determine cybersecurity maturity and identify gaps. Assessment tools include the Automated Cybersecurity Evaluation Toolbox (ACET), FFIEC Cybersecurity Assessment Tool, CISA Ransomware Readiness Assessment, and Cyber Resilience Review (CRR).

One of our first customers was a credit union. Protecting critical infrastructure at small- and mid-sized financial institutions has been a specialty of Blumira from the start. In fact, a driving force behind Blumira is to provide comprehensive cybersecurity protection so organizations can focus on core business objectives like growth, community service, and maximizing value to members.