

5 WAYS TO PREPARE FOR CYBERATTACKS

By John Stream, CISO, SwitchThink Solutions

In the first half of 2021, the financial industry experienced a 1,318 percent increase in ransomware attacks.¹ Cyber criminals targeted credit unions across Canada in June.² These facts prove the question is not *if* a cyberattack will happen, the question is *when*.

Cyber threats and data breaches come in the forms of ransomware attacks, phishing targeted to employees or members that lead to financial scams or data breaches, and more. Social engineering is a form of phishing growing more common where cyber thieves manipulate people into sidestepping security procedures to provide information. The NCUA, Cybersecurity and Infrastructure Security Agency (CISA), FBI, and National Security Agency have issued alerts and advice encouraging credit unions of all sizes to increase cybersecurity awareness and proactively look for threats.³ Credit unions that have taken steps to prepare will be able to respond quicker or avoid attacks.

5 Steps to Take Now

Here are five basic steps credit unions can take to better prepare for cyberattacks.

1. **Assign at least two trusted people to oversee cybersecurity.** Duplication helps with consistency. Professionals with strong data security qualifications are difficult to find and other companies will heavily recruit them.
2. **Build a relationship with your legal counsel** and ensure they participate in your incident response plan. This relationship allows for quicker, more coordinated reactions and protected communication in case of a breach.
3. **Make sure you have a solid incident response plan and playbook** that includes a process to isolate, investigate, and remediate the breach. The NCUA Board proposes a new rule requiring federally insured credit unions to report cyber incidents to the NCUA no later than 72 hours after they become aware of the incident.⁴ To help ensure your credit union is prepared, make sure you have forensics capabilities to add credibility to your response. These steps help ensure your prompt, accurate and transparent reaction.
4. **Test your incident response plan and playbook** at least annually and as significant new threats surface. Prepare for media, members, and others to evaluate and criticize your credit union's response to a cyber incident.
5. **Evaluate the cyber tools you use** to mitigate and respond to cyber incidents. Credit unions need layered defenses and must ensure their tools are continuously monitored. More than 50 percent of attacks start with valid account credentials.⁵ What monitoring do you have in place to detect activity once the attacker is in your environment?

Secure Help You Trust

Many credit unions look to a third party to take on information security responsibilities. Credit union CIOs and CISOs need someone they trust who is 100 percent focused on specialized security and compliance functions their credit union cannot handle on their own. The value is in having this trusted advisor dedicated to security. Third-party providers work on the credit union's behalf. They



provide access to expensive and time consuming to build capabilities including a skilled team and iron-clad infrastructure that gives credit unions additional knowledge, scale and capacity. Credit unions also gain access to 24 by 7 monitoring and antivirus management that enables these tech leaders to share risk with someone else.

We understand CIOs and CISOs often are overwhelmed, especially with fast-changing, headline-attracting topics like cyber risk. We can help guide credit unions through basic best practices. Credit unions that do the basics well reduce overall risk. Don't wait until something happens to find out your credit union and its members are vulnerable. Prepare now.

¹ Tristan Hinsley, "[Cyber Attacks and Credit Unions](#)," Finextra, December 29, 2021.

² Vera-Lynn Kubinec, "[Credit unions across Canada targeted in cybersecurity incident, but no evidence data compromised: tech company](#)," CBC News, June 14, 2022.

³ "[Current Geopolitical Events Increase Likelihood of Imminent Cyberattacks on Financial Institutions](#)," NCUA, January 2022.

⁴ "[Cyber Incident Notification Requirements for Federally Insured Credit Unions](#)," NCUA, July 27, 2022.

⁵ "[Risk and Vulnerability Assessment \(RVA\) Mapped to the Mitre ATT&CK® Framework](#)," CISA.gov, FY21.

About the Author

John Stream has nearly 20 years of experience in advanced data center design and support as an engineer, director, and currently as Chief Information Security Officer for SwitchThink Solutions. He led SwitchThink parent company, Desert Financial Credit Union, through two core conversions that included building resilience and high availability into each solution. Following the conversion to **KeyStone**, John oversaw the design and build of SwitchThink's industry best-in-class, secure client hosting environment. John leverages his infrastructure, networking, systems, security, compliance, and leadership background to oversee security and compliance for SwitchThink's hosted clients, including \$8.4 billion Desert Financial. John holds a computer science degree with a math minor. His certifications include: Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), Payment Card Industry Professional (PCIP), and Certified Data Privacy Solutions Engineer (CDPSE).

About Us

SwitchThink Solutions is an IT Services CUSO formed in partnership with Corelation. As credit union professionals dedicated to optimizing & expanding **KeyStone's** capabilities for our clients, we've developed deep domain expertise in the areas of conversion, development, hosting, & operational best practices. Leverage our knowledge to unlock new strategic possibilities through performance improvement & rapid innovation.

Services include managed & infrastructure cloud hosting solutions; disaster recovery solutions; development & consulting services; conversion support services; & our new SaaS Essentials featuring KeyStone (offering a fully outsourced suite of mission-critical applications to support your enterprise). Whether you're an existing user or preparing for implementation, let our experts help you rapidly apply the transformational powers of **KeyStone** & Cloud Computing. Rethink what's possible with SwitchThink.