RESEARCH BRIEF

Up in the Cloud or Down on the Ground? Cybersecurity Talking Points for Credit Unions

AUTHOR

Linda Young
PonderPickle

15 MINUTE READ

An effective cybersecurity strategy is rarely noticed, but a single failure can cause considerable financial and reputational damage to financial services providers.

OVERVIEW

This research brief summarizes key cybersecurity and associated technologies such as cloud computing that credit union leaders must address now and in coming years. Interviews with credit union leaders and security professionals help identify critical security issues and operational vulnerabilities. The provided talking points will help shift the conversation and action at your credit union toward a stronger cybersecurity strategy.

Fact & Fiction

Since the 1950s, over 100 films have been made featuring hacking and cybersecurity threats. There have been hackers stealing gold from the police and mafia (The Italian Job, 1969), a high school student hacking the military's computer systems (War Games, 1983), the ultimate battle of human vs. machine (The Matrix films, 1999, 2003), and several documentaries featuring infamous cybercriminals (The Great Hack, 2019, The Silk Road, 2021). The cyber battles that play out on film have also been playing out in real life. According to Cybercrime magazine, in 2021 alone, the harm inflicted by cybercrimes is estimated to be $6 trillion. These crimes are forecasted to continue to grow year over year, and by 2025, the damage will reach over $10 trillion. The two industries most vulnerable to cyberattacks are healthcare and financial services. For credit unions, protecting internal assets and members' assets go beyond security dos and don'ts. It is about credit union do's and don'ts, and it is about having the technology talk, but in a different way.

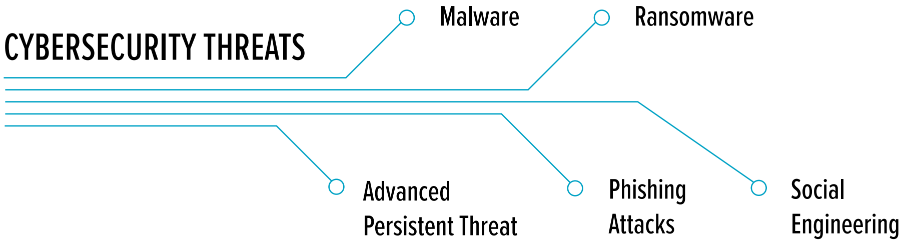
This research brief summarizes key cybersecurity and associated technologies such as cloud computing that credit union leaders must be aware of now and in coming years. A series of in-depth interviews were conducted by the author with credit union leaders, financial services providers, and security firms in April and May 2021. Critical security issues are further illustrated through the experiences shared by credit unions and financial services providers interviewed for this research. Additionally, insights by security professionals who specialize in protecting credit unions and other financial services providers are highlighted. One central element to these interviews involved identifying existing operational vulnerabilities at credit unions when tackling cybersecurity issues. The brief identifies six talking points to help shift the technology infrastructure conversation to better address cybersecurity concerns and associated solutions to tackle security threats at your credit union.

In 2021 alone, the harm inflicted by cybercrimes is estimated to be $6 trillion. These crimes are forecasted to continue to grow year over year, and by 2025, the damage will reach over $10 trillion.

Top Cybersecurity Threats

According to the US Cybersecurity and Infrastructure Security Agency, cybersecurity is "*the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.*" There are several cyberthreats keeping credit union leaders and security experts up at night (Figure 1).

FIGURE 1: Top Security Threats



- **Malware.** Malicious software such as computer viruses, spyware, and Trojan horses (e.g. Emotet, Trojan, 2018—attacking financial data passwords).
- **Ransomware.** Malware that locks or encrypts data until a ransom is paid (e.g. Colonial Pipeline, 2021–shutting down Northeastern US fuel supply).
- **Advanced Persistent Threat.** An attack in which an unauthorized user gains access to a system for a long period of time without being detected; entry may be through malware that appears to be dormant (e.g. Equifax breach).
- **Phishing Attacks.** Obtaining sensitive information (e.g., personal data, passwords, credit card information) through fake email, phone call, or text message (e.g. Fraudulent IRS or COVID scam emails or calls).
- **Social Engineering.** Manipulating an individual's weaknesses to obtain confidential information often combined with phishing (e.g. cyber romance fraud crimes).

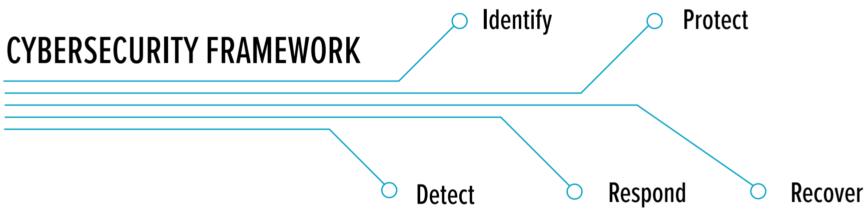
Each of these threats requires several protocols to effectively defend your organization from them. There is no single solution. A comprehensive approach can help mitigate the risks.

The Protective Blueprint

One protective blueprint for these cyberthreats comes in the form of the ***National Institute of Technology (NIST) Framework*** (Figure 2). There are three main components to this framework:

1. **Core–**an organization's cybersecurity activities, outcomes, and information references;
2. **Profiles–**alignment of the organization's objectives, risk appetite, and resources regarding cybersecurity, and
3. **Implementation Tiers–**a qualitative approach to viewing and assessing an organization's cybersecurity risk management activities.

FIGURE 2: NIST Cybersecurity Framework



Source: National Institute of Technology (NIST) Cybersecurity Framework, https://www.nist.gov/cyberframework.

The NIST Framework uses business drivers to guide cybersecurity activities and suggests incorporating cybersecurity risks into an organization's overall risk management process. The Framework provides structure to credit unions looking to improve the security and resilience of their critical infrastructure.

NIST’s Framework also includes five elements to assess preparedness and provide a common taxonomy for organizations to improve.

1. Describe current cybersecurity posture.
2. Describe target state for cybersecurity.
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
4. Assess progress toward the target state.
5. Communicate among internal and external stakeholders about cybersecurity risk.

From a compliance perspective the NCUA launched the ***Automated Cybersecurity Examination Tool (ACET)*** in 2018 which incorporates elements of NIST to assess the cybersecurity maturity level of credit unions with $1 billion+ in assets. Today, the NCUA conducts ACET assessments among all credit unions with over $100 million in assets.

Shifting the Technology Talk

You have heard the analogy of the core banking system being the backbone to a credit union’s operations. Without a strong backbone, a credit union may be challenged to effectively serve its members, tackle the day-to-day challenges of running of a credit union, and achieve its longer-term goals and objectives. With a weak backbone, a credit union may also fall short in responding to various cyberthreats.

Expand upon this analogy and imagine if the entire technological infrastructure at your credit union took shape as a human being. How would you describe the type of person it would be? What is it's stage of life? Perhaps it is an adolescent with a whole lot of attitude but lacking life experience and know how? Or maybe your technology is firmly rooted in adulthood with some experience under its belt and growing responsibilities.

The credit union leaders and security professionals interviewed for this research describe their technology infrastructure as a human being. Direct quotes from the interview can be found to the left. «

“It’s a mid-career professional, ready to leap”

“1999 model in a 2021 world.”

“It’s a young adult with lots of education but little experience.”

“Getting to know who you are... needs to feed a family.”

“Woefully end of life.”

🟦 *Credit Union Leader Quote*
🟥 *Security Professional Quote*

And, how healthy is your "technology person?" Would you describe your technology as young person: strong, nimble, and flexible? Or is it more like an elderly person: weaker and prone to aches and pains? What about its immunity level? Is your technology person susceptible to catching the equivalent of a common cold?

How about the way your credit union learns and applies knowledge in all it does? Is there an attitude of continuous growth and learning with a future focused outlook? Or is there a more closed mindset with an aversion to change and new experiences?

While this characterization of credit union technology infrastructure can be interpreted as light hearted, the intent is anything but. Shifting the way we talk about a credit union's technology infrastructure has real implications to the credit union's overall well-being, especially if the technology and associated infrastructure unintentionally exposes the organization and its members to cybersecurity threats.

The remainder of this brief presents key findings in the form of six talking points to help shift the technology conversation to better address cybersecurity concerns and associated solutions.

TALKING POINTS

#1: Cyberthreats That Conform

Regardless of your size, how cyber savvy is your credit union in preparing for relevant threats?

The types of security breaches faced by credit unions may differ depending on their size. One security professional shared some simple examples to explain the degree of threats. All threats are a danger for all credit unions, however there are some trends. Smaller credit unions may face more malware threats with software infecting files and disrupting operations. This may occur because no one is tasked to regularly check the security of endpoints. For larger credit unions, well-disguised phishing attacks in the form of emails to a credit union's commercial banking staff or accounting staff may appear to be legitimate business correspondences and staff unintentionally share private financial information. The implications for credit unions are to ensure proper processes are in place (e.g., to regularly inspect infrastructural weak points) as well as customize staff security training so it is more relevant to their work and helps to fortify the credit union to respond to new and evolving cyberthreats as their business grows.

"Technology is straight forward but educating staff about security concerns is not so straight forward if there is a culture of technology fear."

"Criminals don't care about your [credit union's] asset size!"

At the same time, regardless of asset size, all credit unions face cybersecurity threats and need to prepare for various degrees of threat. Criminals do not care about your credit union’s asset size. If there is a security opening that is easy to breach, they will take the opportunity.

#2: It’s a Mind Game

How can you remove the fear from your credit union?

What the FUD! When daily headlines are filled with the latest cyberattacks and security breaches, it’s easy to fall into the fear (F) of it all, uncertainty (U) of what your credit union may face, and doubt (D) as to whether your credit union is appropriately prepared if attacked. If a credit union is overtaken by FUD, it may become less confident that it has the knowledge and resources needed to detect, react to, and protect members from cyberattacks.

“I’m not sure whether our team is fully capable of defending us.”

“We are credit union folks, not technology experts.”

“Some [credit unions] bury their heads and think it won’t happen to me."

As the previous talking point outlined, although the types of cyberthreats conform to the stage or size of the credit union, the risks remain a constant. One credit union leader described how employees, from the frontline staff to the c-suite and board directors, need to have a better attitude and be “on board” to take security matters seriously on all fronts. He further explained an existing flawed mindset of prioritizing internal security concerns over external security concerns. Because members are banking and transacting on several fronts, there is the responsibility of credit unions to be an additional external pair of eyes to detect threats on behalf of its members.

How you think about the threats will direct what you do. Fear based thinking will result in poorly thought out, reaction-prone actions.

#3: Do Not Forget About the Business

What business cost is your credit union willing to incur?

When addressing security matters, a framework such as the one provided by NIST is foundational to creating a game plan to protect a credit union from cyberattacks. Some credit union leaders I interviewed discussed the need to ensure business elements are front and center in the desired outcomes of the decision framework. The business decision elements expressed by credit union leaders interviewed included:

- Ensure member experience does not falter and member friction is minimal.
- Speed to market for service delivery should not be impaired.
- Tie back to business continuity planning to ensure a holistic approach to managing risk, including existing preparedness plans and integration with ERM (enterprise risk management).
- Adjust the security posture so the credit union is protected but minimizes employee challenges when something unexpected arises–e.g., the work from home mandate during COVID and allowance for employees to use personal computers until company issued devices are made available.

"If credit unions don't have the controls in place to avoid data breaches, there's a reputational risk because it's a competitive space they are in. Customers can go elsewhere."

"Not technology decisions, only business decisions."

"Something has to give. Can't be 100% compliant all the time."

Financial services is a risk mitigating business and that includes managing cybersecurity risk.

#4: Clouding the Issue

How can your credit union seek understanding and clarify purpose before deciding on cloud-based technology?

Discussions with credit union leaders about cloud-based technology conjure up *myths* such as:

- *It is a cost decision.*
- *It is not as cost effective as you think.*
- *It is about making a decision between a public vs. private option.*
- *It is not secure.*
- *Every credit union is on the cloud already, they just do not know it.*

Leaders would do better to dive deeper and uncover the nuance within these remarks to reveal that cloud-based options are not all-or-nothing

“Cloud computing opens up opportunities for growth for smaller credit unions.”

“Takes the lid off [of current infrastructure limits].”

“Can access what the giants have.”

“[Cloud-based technology provides] access to amazing computing power but [you] pay only for what you use.”

propositions. In fact, accessing cloud-based technology can help credit unions achieve their security and other goals, and multiple tiers of service are often offered depending on a credit union’s needs. Security on the cloud–whether it is a public or private cloud (or hybrid of the two)–is a shared responsibility between the provider and the end user organization. Internal or vendor security administrators are able to set appropriate security levels based on a credit union’s risk appetite.

Discussions about whether to invest in cloud-based technology often elicit uninformed remarks when there is a real variety of available options.

#5: The Knowledge Challenge

How can your credit union fill cybersecurity knowledge gaps?

The challenges faced by interviewed credit union leaders often center on the real and perceived lack of knowledge about how to get ahead of cybersecurity matters, the pros and cons of cloud solutions, and detecting the weaker security elements of their organization’s infrastructure. Impacting this knowledge gap is the need to have the people and structure in place to tackle these challenges.

Smaller credit unions that deem they are not big enough to hire the right talent and commit to the level of resources needed to maintain a team of security employees may be mistaken. I spoke with a leader at a smaller credit union that outsourced its Chief Information Security Officer (CISO) role. This allowed the credit union to ensure they: remain proactive, maintain security standards, accomplish activities, and provide a voice at the table for the work. All without hiring a full contingent of talent.

“Smaller credit unions don’t have IT staff, let alone security staff.”

“We need to build the institutional muscle so even if the talent goes, the credit union can still move forward.”

For larger credit unions, a common internal path that can be followed begins with the security mandate first falling under the IT/technology function and is later moved to enterprise risk with a CISO role independently reporting to the CEO and board. As the organization matures, so does the responsibility for managing knowledge and action around cybersecurity.

There are knowledge gaps in most areas within most credit unions. Gaps in security knowledge are no different.

#6: Two Sides of the Coin

Does this describe your credit union? What solutions can result in both sides winning?

When a coin is tossed, we are asked to call heads or tails. Yet, it is the same coin regardless of the outcome of the coin toss. One credit union leader challenged this zero-sum game toss where one side is serving members while the other side is addressing various types of risks, including cybersecurity risks. Does mitigating risk have to be done at the expense of the member? Does serving members well mean taking on more risk? Furthermore, if there is a "we don't know what we don't know" mentality when it comes to cyberthreats, wouldn't it be the same "don't know" issue when it comes to the member impact?

Moving away from this either/or coin toss can free credit unions to be more holistic in their solution identification and assessment, and better understand how actions can impact multiple factors in nuanced ways.

Having to choose between the member side of the coin or the risk and security side make for a winner/loser outcome.

"I'm there as a technology leader to represent the member. What problem is technology trying to solve on behalf of the member?"

"My expectation is [that] service is never down for members and this includes services offered by our vendors."

"Don't think you can address the cyber concerns without addressing the member concerns. You're not on an island."

CREDIT UNION IMPLICATIONS

Recharge Your Cybersecurity Discussions

To plan and execute cybersecurity efforts that make a sustainable and positive difference in the long run, credit union leaders must not fall back on the usual discussion points raised when discussing cybersecurity concerns, budgets or proposed plans. Instead, consider the subtle or not so subtle opportunities to shift the conversation toward more productive talking points and recharge your cybersecurity efforts.

Talking Point #1 ***Cyberthreats that Conform***	Criminals do not care about your credit union's asset size. If there is a security opening that is easy to breach, they will take the opportunity. *Regardless of your size, how cyber savvy is your credit union in preparing for relevant threats?*
Talking Point #2 ***It's a Mind Game***	How you think will direct what you do. Fear based thinking will result in poorly thought out, reaction-prone actions. *How can you remove the fear from your credit union?*
Talking Point #3 ***Don't Forget about the Business***	Financial services is a risk mitigating business and that includes managing cybersecurity risk. *What business cost is your credit union willing to incur?*
Talking Point #4 ***Clouding the Issue***	Discussions about whether to invest in cloud-based technology often elicit uninformed remarks when there is a real variety of available options. *How can your credit union seek understanding and clarify purpose before deciding on cloud-based technology?*
Talking Point #5 ***The Knowledge Challenge***	There are knowledge gaps in most areas within most credit unions. Gaps in security knowledge are no different. *How can your credit union fill cybersecurity knowledge gaps?*
Talking Point #6 ***Two Sides of the Coin***	Having to choose between the member side of the coin or the risk and security side make for a winner/loser outcome. *Is this characteristic of your credit union? What solutions can result in both sides winning?*

THANK YOU

A special thank you to Think | Stack for making this research possible.

THINK STACK

filene.org/542