CUNA MUTUAL GROUP

RISKS AS YOU GROW

What you should know about protecting your credit union's data

Cybersecurity is one of the most dynamic risks to manage. In fact, an analysis of the cybersecurity strategies and executions plans of 4,000+ companies revealed that 73% are not adequately prepared to face a cyberattack.[1]

Cybersecurity is more than an IT problem

Credit unions are responsible for protecting their own data and their members' data. Cybersecurity is often thought of as a backend IT process, but it is actually a strategy that should be supported all the way from the c-suite to every staff member in your organization. Learn about the key threats to data security and what your credit union can do to minimize risk.

Threats in the cyber landscape

"Cyberattack" is a threatening term, but it is actually a vague word that could refer to any number of vulnerabilities and security risks. Do not assume your IT team has all of those threats under control. Educate yourself and every employee of your credit union on how to recognize and approach the key cybersecurity vulnerabilities.

3 Main Threats
Confidentiality
Integrity
Availability

The different type of threats

Here are the three main threats and how they could affect your credit union's data and your members' data.

- **Confidentiality.** If the confidentiality of data is breached, this means it has been stolen or copied. Phishing attacks are a common method of breaching data's confidentiality, or privacy. The perpetrator of a phishing attack will pretend to be a trusted person or entity and asks for permission, often via email or text, to access your data or your members' data and install malware.
- **Integrity.** The integrity of your data refers to its accuracy and safety. Perpetrators of a data integrity breach aim to alter, corrupt, or even completely destroy data or complete information systems. This type of attack often has no monetary motivation. Instead, it is a type of digital vandalism.
- **Availability.** Data availability refers to your ability to access it. Ransomware and distributed denial-of-service (DDoS) attacks are two common methods of compromising data availability. If your credit union is hit with this type of attack, you may be unable to access a portion or even all of your data. The perpetrator will likely try to demand some type of payment – typically in Bitcoin or another type of cryptocurrency – to release the data.

An analysis of the cybersecurity strategies and executions plans of 4,000+ companies revealed that 73 percent are not adequately prepared to face a cyberattack.[1]

1 *Hiscox Cyber Readiness Report 2018*

2 *2018 Data Breach Investigations Report Verizon, 2018. Web. 14 May 2018.*

Insider threats vs. outsider threats

Threats to data confidentiality, integrity, and availability can come from both outside and within your credit union. The majority of cybersecurity threats (73 percent) are external, while just 28 percent involved internal actors.[2] The threat pattern may be different, but most motives (93 percent) are related to financial gain when the attack involves financial institutions.[2] Here are some of the most common insider and outsider threat actors.

Insider threats

- **Employees, Volunteers and Contractors.** Employees, volunteers like your board members, and contractors have access to your credit union's data and member data. Unintentional errors, like opening and downloading an email that contains malware, is one of the most common insider threats. But, an insider can also intentionally compromise the confidentiality, integrity, and/or availability of that data. For example, an employee or contractor could steal data by downloading it to a USB flash drive or to a personal account. Insiders can be financially motivated, but they may also be seeking revenge or professional advantage.

  Employee training is vital to mitigating losses due to error. Minimize malicious employee breaches by limiting data access, encrypting data when it leaves your network, and monitoring for any suspicious activity.
- **Vendors.** Credit unions work with a significant number of third-party vendors that have access to their data and member data. These vendors are vulnerable to all the same types of cybersecurity threats – external and internal – your organization is, but they may not always have the same protections and strategies in place.

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

$8.76 MILLION

is the average cost of cybersecurity incidents caused by company insiders[3]

Understand which of your vendors have access to your data, ask your vendors how they protect your data, and consider putting security requirements and risk oversight in place to best manage organizational resources on your behalf. Your third-party relationships are only as strong as their weakest link.

The annual cost of cybersecurity incidents caused by company insiders is $8.76 million, according to The Ponemon Institute's report.[3]

Outsider threats

- **Cybercriminals.** Cybercriminals, also commonly referred to as hackers, are most likely to target financial and personnel information using keystroke loggers, Trojan viruses, phishing emails, and malware. A cybercriminal can be a single person working alone or part of a larger organization. Cybercriminals typically look for easy targets to attack. In recent years, they have shifted from individual consumers to businesses and their employees.
- **Nation-states.** Cyberattacks can be state-sponsored. When a nation-state sets out to breach an organization's data security protocols, common motivations are political or the gain of intellectual property.
- **Hacktivists.** Hacktivists are driven to steal or compromise data in the name of social or political movements. Anonymous is a well-known hacktivism group known for perpetrating DDoS attacks against government, corporate, and religious organizations.
- **Industrial cyberspies.** Cyberspies are agents of corporate espionage. They are interested in acquiring intellectual property or inside information on competing companies to gain an advantage.

3 *2018 Cost of Insider Threats: Global Organizations The Ponemon Institute, 2018*

Conclusion

Arming yourself with the knowledge of the variety of cyber threats active today will help your credit union minimize its risk.

Next-gen vulnerabilities

Cybersecurity strategies are evolving quickly, but so are threats to data security. New technologies are emerging, and savvy threat actors are constantly looking for ways to find and exploit vulnerabilities. Credit unions need to stay on top of next-generation vulnerabilities to minimize risk and prepare a response for potential loss of information and data.

Cryptocurrencies

Cryptocurrency is a type of digital currency that is transferred using a peer-to-peer system, which means an algorithm keeps track of all transactions, rather than a central bank or government. Blockchain, the technology that makes cryptocurrency possible, is the decentralized ledger that tracks and validates cryptocurrency transactions.

You likely know Bitcoin is a type of cryptocurrency, but there are a number of other varieties such as Litecoin and Ethereum.

Credit unions should know the basics of cryptocurrencies because they are the preferred means of payment for ransomware attacks. The

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

anonymous nature of cryptocurrency transactions makes cryptocurrencies an attractive medium for this type of digital extortion. In addition, threat actors do not need to know how to create ransomware. They can simply pay for it with Bitcoin, send it, and profit. The ease of enacting this threat will likely make it increasingly common.

If your credit union falls prey to a ransomware attack that demands Bitcoin or another form of cryptocurrency payment to regain access to your data, you need to know if, when, and how to respond. Time is limited in these situations.

Knowing the answers to the following questions can help your credit union in the event of a ransomware attack.

- Can you try to restore your information system and bypass the ransomware demands?
- Can you afford to lose the data being ransomed if you do not pay?
- If you are going to pay, how do you get enough Bitcoin within the demanded timeframe?
- And, are you really guaranteed to have your data returned even if you pay?

Responding to ransomware comes with tough business decisions, but ones your credit union must make based on your own individual circumstances.

You also need to be aware that your credit union may not be the sole target of this type of attack. Threat actors may target multiple credit unions at once. For example, a threat actor could find and exploit a vulnerability in software that the majority of credit unions use and try to affect the majority of the space through that one weakness.

Like many legitimate investors, cybercriminals have also recognized the potential opportunities of cryptocurrency. So much so, that cryptomining-malware has been reported as the top cyber threat in 2018.[4]

Cryptocurrency mining is the process in which cryptocurrency transactions are verified and then added to the blockchain ledger. The first miner to crack a mathematical code during the verification process is rewarded with a small amount of cryptocurrency. Mining can be profitable, if the rewards outweigh the hardware and energy costs required to complete the complex mathematical equations associated with verification.

Cryptomining malware has been reported as the top cyber threat in 2018.[4]

Cryptojacking entails the unauthorized use of a computer system or mobile device to mine cryptocurrency through cryptomining-malware. As opposed to ransomware, cryptojacking does not target a victim organization's data. However, it does steal CPU processing power.

Cryptocurrencies: What your credit union can do

Should a credit union have multiple systems cryptojacked, financial damages in terms of business interruption, slower processing time, and the need

4 *April's Most Wanted Malware: Cryptomining Malware Targeting Unpatched Server Vulnerabilities, Check Point, 2018. Web.*

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

to replace infected hardware may be incurred. Like many cyber risks, the two primary methods of infection are through phishing attacks and malware-infected website pop-ups.

Knowing how to respond ahead of time is crucial in minimizing risk and protecting your credit union's reputation. In fact, an effective incident response plan is essential to minimizing the impact of a security incident and allowing the organization to return to normal as soon as possible. These preparedness efforts can ensure actions are taken in a coordinated, controlled manner.

Being prepared for cyberattacks, cryptocurrency demands, and cryptojacking will only grow in importance. Cryptocurrency is making it increasingly attractive to get into the business of cybercrime. Bitcoin is legal, widely used, and primarily unregulated. It is also possible that hackers could compromise investment programs and steal cyrptocurrency.[5] Without clear regulations and legal process, regaining cryptocurrency after you've been defrauded could also be extremely problematic.

Back-end security protocols, commitment to employee training, and an effective response strategy are all critical to minimizing your risk of cryptocurrency-driven attacks.

Internet of Things

The Internet of Things (IoT) is rapidly becoming ubiquitous. Businesses and homes are being filled with smart devices. ATMs, smartphones, clocks, televisions, appliances, medical devices, and more are a part of the IoT. Intel estimates that the global value of IoT technology could reach $6.2 trillion dollars by 2025.[6] By next year, 85 percent of organizations will have adopted IoT technology.[7]

This increased connectivity makes our lives much easier and our business more efficient in many ways, but the IoT also opens the door to a flood of potential cybersecurity issues. The rapid rate at which these IoT devices are being deployed often means rigorous security protocols are left behind.

Cybercriminals are well aware of the opportunity presented by the IoT and lax security. Your credit union likely has IoT devices connected to your network. Additionally, employees and members bring in devices that can potentially connect to your network. Each is a potential entryway into your network and the sensitive data it stores.

Approximately three in five businesses can trace some type of security incident back to their use of IoT devices.[8] The IoT is vulnerable to malware, phishing attacks, ransomware attacks, and more.

Despite the growing concerns around the IoT, many organizations are not making the IoT a cybersecurity priority.

- **Just 28 percent of organizations label their IoT cybersecurity strategy very important.[8]**
- **Less than half of organizations (49 percent) have IoT patching policies.[8]**
- **Only 47 percent of organizations regularly analyze the risk posed by third-party use of IoT devices.[8]**

Internet of Things: What your credit union can do

Preparation and education are the best approaches to minimizing any kind of security risk. Reduce your cybersecurity risks related to the IoT by following these steps:

5 *Cryptocurrency Fraud Widespread, Warns Regulatory Forbes, 10 April 2018. Web. 29 May 2018.*

6 *A Guide to the Internet of Things Intel. Web. 17 May 2018.*

7 *Internet of Things Hewlett Packard Enterprise, 2018. Web. 17 May 2018.*

8 *Internet of Things Cybersecurity Readiness Trustwave, 2018. Web. 17 May 2018.*

- **Know your devices.** Before you can form an IoT cybersecurity strategy, you need to know what devices are in your credit union. In addition to your own devices, what devices brought in by employees and members – like wearables – could potentially connect to your network?
- **Understand how these devices communicate with your network.** You likely know which devices connect to Wi-Fi in your credit union. What about Bluetooth connectivity? What about connecting to the cloud? Connectivity has varying levels of complexity and varying levels of network access.
- **Know what security you have in place.** Does your existing approach to cybersecurity include the IoT? Does your credit union install security patches for connected devices in a timely manner? Review your policies to make sure you are paying an appropriate amount of attention to the IoT and the potential associated risks.
- **Assess your data collection policies.** A breach of member data does considerable damage to a credit union's reputation, as well as financial damage. Carefully assess how devices are storing data and what data is being stored. The privacy risks associated with the collection of IoT data may present itself from the collection of member personal information, spending habits, and physical locations.

Cloud computing

The terms "cloud" and "cloud computing" are floating around everywhere. In fact, nearly all organizations, both public and private, (97 percent) use cloud services.[9]

There are three main types of cloud computing.

- **Software-as-a-service (SaaS).** SaaS is a common cloud solution for businesses. SaaS means a business will buy a software application subscription and access the software via the internet.
- **Infrastructure-as-a-service (IaaS).** IaaS refers to a model where a cloud service provider hosts a number of infrastructure components that are available for other businesses to use.
- **Platform-as-a-service (PaaS).** PaaS is a form of cloud computing that allows businesses to custom build and manage the applications they need.

25%

of organizations have had data stolen from the public cloud.[9]

The cloud is increasing in popularity because it cuts down on infrastructure costs, it is not affected by hardware failures, and it allows users a high level of flexibility and connectivity.

Why is it a cybersecurity issue? Any method of data storage, including the cloud, presents a cybersecurity issue. Here are a couple of key statistics to know.

- One in five organizations has detected attacks against their public cloud.[9]
- 25 percent of organizations have had data stolen from the public cloud.[9]

Cloud computing capabilities are expanding so quickly that security often lags, and cybercriminals are exploiting that disconnect to attack and breach the cloud. They can manipulate legitimate cloud services to introduce malware into a network. The use of legitimate services can make it difficult to detect these attacks.

The cloud is also vulnerable to a whole host of

9 *Navigating a Cloudy Sky: Practical Guidance and the State of Cloud Security McAfee, 2018. Web. 18 May 2018.*

typical cybersecurity threats such as data theft, DDoS attacks, and phishing scams.

Cloud computing: What your credit union can do

Here are four ways your credit union can address the cloud in their cybersecurity strategies.

- **Manage data access.** Who has access to the data stored in the cloud? How is that access managed? How can you detect unauthorized access? Knowing the answers to these questions helps protect your data and your members' data from malicious external and internal threats.
- **Enable security measures that can scale.** Scalability is one of the main benefits of the cloud, but you leave the data stored there vulnerable if you cannot scale your security solutions with it. Use layered measures, like encryption, that make exploitation and theft more difficult to execute.
- **Conduct regular risk assessments.** Credit unions cannot minimize cybersecurity threats to their cloud if they do not know what those threats are. Determine what your risks are and put the appropriate safeguards in place.
- **Know your cloud provider's approach to security.** Cloud service providers are major cybercriminal targets. This means your data is on the line if and when your service provider experiences a cybersecurity incident. Know what security they have in place to prevent the loss or compromise of data, and know their level of accountability if that does happen.

GDPR

The European Union's (EU) General Data Protection Regulation (GDPR) recently went into effect, causing financial institutions to scramble to comply. However, some aspects of the regulation are still unclear, leaving many credit unions with the same questions.

GDPR regulates the processing of personal data including the collection, storage, transfer, and use of the data. Basically, any information that can be used to identify an individual is considered personal data. Personal data includes, but is not limited to:

- Name
- Email address
- Medical information
- IP address
- Location
- Financial Institution details
- Physical Information
- Genetic data

The GDPR is a set of data privacy regulations put in place by the EU. The new law, which has a total of 99 articles,[9] went into effect on May 25, 2018. The law is geared toward consumer protection, but the process of becoming compliant can be cumbersome and expensive for businesses.

GDPR: What your credit union can do

While GDPR focuses on the rights of individuals in the EU, the impact will extend to organizations and companies worldwide. GDPR applies to companies,

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

Privacy is a risk-based problem

GDPR gives individuals control and ownership over their personal data. Organizations, beginning with the c-suite, should assess which data privacy and security risks they face and determine their risk tolerance. Privacy risks typically are financial (such as fines and lawsuits) and reputational (bad press and negative perceptions). But GDPR also introduces risk around an individual's data rights and requests.

GDPR is comprised of 99 articles, each with multiple subcomponents making it extremely dense and vague, without exact guidance on how to comply. However, GDPR preparation can be achieved if your credit union has a good data management approach and a well-documented plan in place.

If your credit union is subject to GDPR, there are strict reporting requirements if a breach occurs. GDPR does not differentiate between accidental and intentional breaches when it comes to reporting requirements. Any security breach involving personal data must be reported to the credit union's EU supervisory authority within 72 hours. The 72-hour countdown begins at the time of detection.

In addition, in certain cases, members whose personal data has been compromised must be notified in an expedited manner. This would include scenarios where there has been theft, loss, or damage of personal data.

Clearly, the aim of the GDPR is to ensure that an individual's personal data is processed with consent, for a specific purpose, and for a reasonable amount of time. However, some aspects are unclear, leaving many credit unions unsure whether they fall within the jurisdiction of GDPR.

financial institutions, and government agencies/ entities of any size.

If your credit union has at least one branch in the EU, EU authorities could determine that GDPR applies because you have a physical presence in the EU. Nonetheless, GDPR also may apply to credit unions without a physical presence in the EU, if a credit union processes the personal data of someone in the EU.

Unfortunately, determining exactly when GDPR applies may be difficult until enforcement actions are issued and litigated. ***If you're uncertain about whether GDPR applies to your credit union, don't make that determination until you've consulted with your attorney.*** For those subject to GDPR, it is essential to continually assess how your credit union processes and protects your members' data.

The fines for non-compliance are considerable. There are a total of 10 criteria used to determine the fine amount. The first tier is 2.00% of annual revenue or €10 million, whichever is greater. The second tier, for more severe non-compliance, is up to 4.00% of annual revenue or €20 million, whichever is greater.

Conclusion

Cryptocurrency, the IoT, cloud computing, and GDPR are realities of doing business today. Credit unions should stay on top of how these technologies and guidelines are being used and their associated risks.

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

Six key considerations to strengthen your risk posture

Cybersecurity is first and foremost a risk management policy. Credit unions do need to know how to respond in case data is compromised, but mitigating the risk of an incident should be your frontline strategy. Here are six essential ways to strengthen your cybersecurity risk posture.

1 Increase awareness

Staying educated on cybersecurity risks and risk management strategies is the foundation of protecting your credit union's data and information systems. Here are three ways to stay on top of cybersecurity through awareness.

- **Make cybersecurity a part of your credit union's culture.** Every employee of your credit union should be an active part of your approach to cybersecurity. Set aside time and resources for training. Make it clear that protecting your credit union's data is a collective effort, not just the responsibility of a few employees.
- **Keep on top of emerging threats.** Do not become complacent and assume your cybersecurity policy addresses the biggest pitfalls. Threat actors are constantly seeking new vulnerabilities and methods to steal and manipulate data and information systems. Cybersecurity strategy must evolve to keep up with emerging hazards.

  Know how hackers will manipulate the growing use of technologies like the cloud and the IoT. Know the new strains of malware and ransomware gaining traction and popularity amongst hackers. Use the power of knowledge to remain nimble and proactively adjust your cybersecurity policies.

Create a culture of engagement and accountability to minimize the cyber risks and opportunities cybercriminals take advantage of every day.

- **Use the resources at your disposal.** Cybersecurity is a global issue. Your credit union is not alone in searching for ways to protect data and to stay ahead of internal and external risks. Look outside of your own four walls for resources that can help you stay aware and manage your risk.

2 Develop engagement and accountability

Cybersecurity needs to run horizontally through your entire credit union. It is not just an IT problem. Every single staff member, regardless of department and status, needs to be engaged and held accountable. Anyone can mistakenly expose credit union or member data to risk. Create a culture of engagement and accountability to minimize the cyber risks and opportunities cybercriminals take advantage of every day.

- **Engagement needs to start with the c-suite.** Regardless of the roles, everyone in the c-suite needs to be committed to cybersecurity. More than half of c-suite executives (65 percent) believe their cybersecurity strategy is well-positioned, but just 17 percent of these strategies are considered at the highest level.[10]

  With so much at stake, cybersecurity must be a top-tier risk that receives the full attention at your credit union. Engage the c-suite by putting cybersecurity on the agenda.

10 *Securing the C-Suite: Cybersecurity Perspectives from the Boardroom and C-suite IBM. Web. 21 May 2018.*

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

C-suite engagement

Active engagement at the c-suite level will help executives gain a clearer perspective on how effective their data security plans are and what needs to be done to make improvements. Data breaches are expensive and damaging to companies' reputations, which are far-reaching consequences that will reach the c-suite. Cybersecurity is the preparation that minimizes those financial and image risks. C-suite leaders need to actively engage with and guide that strategy so it becomes a part of your credit union's fabric.

- **Establish guiding principles for a successful strategy.** Your c-suite must ensure that your cybersecurity roadmap connects with and supports your credit union's long-term goals. By establishing a sound framework of proactive assessments, policies, and procedures, you will be more likely to protect, monitor, mitigate, and withstand a wider array of threats.
- **Find ways to promote accountability.** A total of two out of five non-executive directors and executives reported they do not feel responsible for the consequences of a cybersecurity attack in a survey of more than 1,000 respondents.[11] Accountability should start at the highest levels and reach everyone in the organization. Commit to finding ways to educate everyone at your credit union about the core elements of cybersecurity, key threats, and how every individual plays an important role in safeguarding your members' data. The challenge is how to get everyone engaged.
- **Invest in training.** It takes a village to be prepared for the entire spectrum of cyber risks and vulnerabilities. Almost half of employees (45 percent) do not receive any form of cybersecurity training from their employers.[12] Credit unions cannot expect employee engagement and accountability if they do not give them access to the right procedures, tools and knowledge. Some of the most common employer-sponsored cybersecurity training methods include online modules (32 percent), in-person workshops (26 percent), paper-based (15 percent), and one-on-one training (14.5 percent).[12] Find a method that works for your credit union and empower your employees to actively participate in cybersecurity strategy.

Cyber risks are one of the best examples of the need for cross-functional thinking to anticipate issues and tackle risk management problems throughout your credit union.

3 Explore new tools and solutions

While threat actors may be busy looking for ways to compromise information systems and steal data, credit unions do not have to be defenseless. New technology is emerging to help organizations bolster their cybersecurity strategy and minimize the risk of cyberattacks.

- **Blockchain.** Blockchain, the technology that makes cryptocurrency possible, will likely be a game changer for cybersecurity, particularly in the financial sector. Blockchain uses a decentralized data storage structure, rather than keeping data all in one place. This makes it more difficult for cybercriminals to access, compromise, and steal that data.

  Blockchain is also driving a shift away from traditional passwords, which have an element of vulnerability due to human error. People may lose

11 *The Accountability Gap: Cybersecurity and Building a Culture of Responsibility Information Security Buzz, 16 April 2016. Web. 21 May 2018.*

12 *Cyber Secure: A Look at Employee Cybersecurity Habits in the Workplace CompTIA, 26 October 2015. Web. 21 May 2018.*

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

passwords or select passwords that are not very secure. With blockchain, users can get a type of secure, digital authentication that is much less prone to manipulation or breaches.

- **Artificial intelligence and machine learning.** Artificial intelligence (AI) refers to a machine's ability to mimic the natural intelligence of living things. Machine learning is a type of AI that refers to a computer's ability to use data to become progressively more successful at a particular task without being taught to do so. Essentially, the machine is learning through experience, like a person would. AI and machine learning means information systems can learn to play an increasingly active part in improving the recognition and deterrence of threats. As a cybersecurity tool, machine learning uses special data and algorithms to identify risks and develop solutions, providing a more-informed response than traditional rule-based security programs.
- **User analytics.** User behavior is a major threat to cybersecurity. Whether unintentionally or with malicious intent, a user can compromise a credit union's data. Curating user behavior analytics can help organizations better understand how users legitimately interact with their information systems and data versus how a malicious attacker would behave.

The cybersecurity talent shortage is a reality, and credit unions will need to find inventive ways to hire the right people to protect their data.

The potential of user analytics

User analytics have the potential to increase early threat detection. For example, analytics could recognize that a user is behaving differently than in the past, which could indicate his or her credentials have been compromised and are being used by someone else. Analytics could also catch malicious behavior by comparing how users within the same part of an organization act within an information system. If one user's behavior stands out, it could mean he or she is an inside threat or someone has stolen those credentials.

While much is being done to combat these attacks, credit unions must learn to be nimble and prepare for how the next generation of technology will impact cybersecurity. A solid security strategy will use multiple tools that work together to protect your credit union's data and reputation.

4 Address the talent shortage

There could be an information security workforce shortage of 1.5 million by 2020, and 45 percent of hiring managers are struggling already to find candidates to fill information security positions.[13] The cybersecurity talent shortage is a reality, and credit unions will need to find inventive ways to hire the right people to protect their data.

- **Invest in employee development.** Cybersecurity does not just have to be about IT. Look to the

13 *(ISC)² Global Information Security Workforce Study (ISC)² Foundation, 17 April 2015. Web. 22 May 2018.*

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

49%

of organizations reported that they have had a data breach caused by a vendor.[14]

people who already work at your credit union, regardless of their current role. Does anyone have an interest in technology and/or a strong curiosity for problem-solving? Recognize that interest and foster it. Credit unions can go a long way toward filling the talent gap by providing employee development programs for cybersecurity.

Career development options appeal to employees looking to add new skills or find ways to bring outside interests into the workplace. Staff members who can understand your operations and processes have the ability to quickly pick up technical skills through on-the-job training. Job shadowing is a good way to build your cybersecurity bench. Plus, this helps bolster your credit union's cybersecurity talent pool without even having to look outside your organization.

- **Rethink recruitment strategies.** Traditional hiring methods are not the only way to find the cybersecurity professionals you need. Instead of casting a wide net, try some more specific recruitment tactics. Post to technology-specific online job boards. Go to tech school and community college job fairs. Try to find candidates through organizations that offer cybersecurity certificate programs. Get involved with middle schools and high schools to teach younger students about the importance of cybersecurity and future job possibilities.
- **Look outside of your credit union space.** Limiting your candidate pool to people who have only worked in the financial sector will only compound the cybersecurity shortage. Instead of focusing solely on banking experience, widen your search criteria to include all different kinds of industries. A talented cybersecurity candidate can learn the ins and outs of working at a credit union on the job. Hire for information security talent and provide on-the-job-training and rotational assignments to address any gaps in knowledge.

5 Manage vendor relationships

Third-party vendors are an essential part of doing business, but they do extend the risk of the exposure and misuse of your credit union's data. Almost half of organizations (49 percent) reported that they have had a data breach caused by a vendor.[14] Managing your own risk as well as the additional risk introduced by working with vendors can be challenging, but carefully managing those relationships can help reduce your credit union's vulnerability to cyberattacks and breaches. Here are five vital steps for managing those relationships.

- **Know your vendors.** It may seem simple, but your credit union should have an easily accessible list of all third-party vendors and what type of access they have to your data and member data. Having this basic information will help you understand your third-party risk and how you should go about managing the relationship. Ensure that this list is maintained and regularly updated.
- **Take necessary steps to understand your vendors' data security standards.** When applicable, contractually require adequate protection of member information and review appropriate security documents to ensure compliance. Due diligence performed on an outsourced service that will not have access to

14 *Data Risk in the Third-Party Ecosystem BuckelySander and Treliant Risk Advisor, April 2016. Web. 22 May 2018.*

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

your credit union network, not have access to member personal identifying information (PII), and not heavily regulated will not be as deep as the due diligence performed if it has network access and is heavily regulated.

- **Know your vendors' cybersecurity strategies.** Less than half of organizations (48 percent) have a vendor risk management committee.[14] If your third-party vendors are entrusted with your credit union's data and its members' data, their cybersecurity strategy is just as important as your own. What safeguards do they have in place to lessen the risk of a breach of your data? Ask that question on a regular basis. Threats to cybersecurity evolve and so should your vendors' risk management.

  Second, you should know your vendors' policies on reporting data breaches. More than a third of organizations (37 percent) believe that a vendor would not inform them if a data breach involving their data occurred.[13]
- **Set expectations for your vendor relationships.** If vendors do not share their cybersecurity policies or those policies are insufficient, consider searching for a different vendor. When making relationships with new third-party vendors, make cybersecurity a part of the vetting process.
- **Know your risk.** If a third-party vendor does experience a breach that affects your credit union's data, what is your risk exposure? A third-party breach could affect your credit union's reputation, compliance, and more. Be aware of those risks so they can be lessened and managed appropriately.

Credit unions should establish processes to evaluate and manage associated third-party risks before entering, during, and even after the vendor relationship ends. Remember, third-party and vendor risk management is an ongoing process.

6 Consider your insurance options

"Purchasing cyber insurance does not remove the need for a sound control environment. Rather, cyber insurance should be a component of a broader risk management strategy."[15] The Federal Financial Institutions Examination Council (FFIEC) recently emphasized the role cyber insurance can play in risk management programs.[14] Here are a few important things to know.

- **Understand the difference between first-party and third-party coverage.** The scope of cyber insurance varies. First-party cyber insurance covers a wide variety of expenses related to a cyber-incident. This type of policy may cover cost related to business disruption, member notification, and extortion.[14] Third-party coverage focuses on claims made against the financial institution by third-parties, such as vendors and members.
- **Policy provisions can vary.** Policyholders should work with their insurance provider to understand key terms and provisions so your credit union is not caught by surprise at the time of loss. In addition, be clear that you've diligently determined the sufficiency of existing insurance coverage and limits as cyber risk exposures and explored a variety of insurance products as the threat landscape continually evolves.

15 *Joint Statement: Cyber Insurance and Its Potential Role in Risk Management Programs Federal Financial Institutions Examination Council, 13 April 2018. Web. 22 May 2018.*

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

- **Understand your provider's response and services.** Know the role that the insurance provider will play in supporting your organization at the time of a breach or loss. Cyber insurance providers can also open the door to invaluable resources and dedicated expertise in preparing for, handling, and responding to cybersecurity risks and incidents.
- **Taking a strategic approach to managing risk at your credit union starts with awareness.** When everyone in your organization is educated, you can focus on engagement, new tools, finding new talent, managing third-party vendor relationships, and selecting the right insurance coverage for your credit union.

Conclusion

Cybersecurity is one of the most dynamic risks for organizations to manage. And unfortunately, only 42 percent believe their company is extremely or very effective at managing cybersecurity.[16] To assist your credit union, commit to understanding the basics of cyber threats, educate everyone from the c-suite down on next-generation vulnerabilities, and embrace key considerations for strengthening your risk posture.

CUNA Mutual Group is dedicated to help you understand these pressing risks and provide you with the most relevant resources you need to build a strong cybersecurity strategy and make confident decisions.

16 *Global Risk Management Survey, 10th Edition Deloitte, 2 March 2017. Web. 29 May 2018.*

17 *Stay Safe Online National Cyber Security Alliance. Web. 21 May 2018. https://staysafeonline.org/ncsam/*

Additional resources

In October, the Department of Homeland Security and National Cyber Security Alliance hold the National Cybersecurity Awareness Month (NCSAM).[17] The entire month is aimed toward cybersecurity education and engagement. Take advantage of the resources this event features – everything from tips on basic internet safety to more sophisticated insight into protecting your infrastructure. Consider developing your own awareness campaign with credit union employees and/or members.

CUNA Mutual Group, cybersecurity insurance carriers, credit union associations and leagues also release free resources on emerging threats – like RISK Alerts, whitepapers, webinars, and risk assessments. These resources provide your credit union with actionable risk management techniques. In fact, you can use these types of resources as a launching pad for education and your credit union's customized cybersecurity approach.

Access the Protection Resource Center (UserID/Password required) at cunamutual.com/prc for exclusive cyber risk and security resources:

- GDPR Risk Overview
- Cloud Computing Risk Overview
- Internet of Things Risk Overview
- Ransomware Risk Overview
- Member Protection Tips
- NIST Cybersecurity Framework
- Post-Breach Consumer Tips
- Vendor Management Risk Overview

Interested in learning more about protecting your credit union's data?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com.

Reach out to the
CUNA Mutual Group
Risk & Compliance Solutions at 800.637.2676
or riskconsultant@cunamutual.com
to gain additional insights about cybersecurity vulnerabilities, protections, and access to more resources to help you rise above the risk.

800.356.2644 | cunamutual.com
P.O. Box 391 | 5910 Mineral Point Road
Madison, WI 53701-0391

CUNA MUTUAL GROUP