2020 eBook Series

Rise Above Your Risk

Cybersecurity Threat Outlook

Including just-in-time insights:

COVID-19 outbreak re-introduces and re-prioritizes cyber risks

Risk & Compliance Solutions
800.637.2676
RiskConsultant@cunamutual.com

CUNA MUTUAL GROUP

Cybersecurity Threats On The Radar

Pressure continues to increase on all fronts.

Awareness of cyber threats has grown rapidly driven by the reliance on data, IT systems, and a number of high-profile incidents. Credit unions also face a growing number of challenges including an increase in ransomware, business email compromise incidents, the prospect of litigation, and a shortage of qualified talent to keep your credit union cyber-secure. Not to mention trying to keep track of how your vendor / partners are caring for and using your member's data.

Three Main Threats to Data Security

Cybersecurity strategies are evolving quickly, but so are threats to data security. 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.

Typically, threats to data security fall into these three categories:

CONFIDENTIALITY

If the confidentiality of your data is breached; it has been stolen or copied. Phishing attacks are a common method of breaching data's confidentiality or privacy.

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.

AVAILABILITY

Data availability is your ability to access it. Ransomware and distributed denial-of-service (DDoS) attacks are two common methods of compromising data availability.

Cybersecurity Threats On The Radar

Cybersecurity is one of the most dynamic risks for organizations to manage. To assist, commit to understanding the ins and outs of cyber threats, educate everyone from the C-suite down on the next-generation vulnerabilities, and embrace key considerations for strengthening your risk posture across the entire organization.

consider these 7 cyber risks

Ransomware

2019 marked a major turning point in which ransomware became more common and far more damaging. In some cases, ransomware developers will now actually publicly release a victim's data – rather than just threaten - if the ransom is not paid.

Mobile Device Technology

With more than 50% of Internet traffic coming from mobile devices, many attackers have turned their fraudulent assaults to remote employees, apps, and mobile devices complete with corporate data.

Source: StatCounter, 2019

Third-Party Relationships

While third-party vendors are essential to business, hackers are increasingly targeting vendor vulnerabilities to access organizations' data. In fact, 56% of organizations attribute data security issues to vendors or other third parties.

Source: Data Risk in the Third-Party Ecosystem, Ponemon and Opus, 2018

C-suite Engagement & Governance

Cybersecurity should be part of your fabric and culture – firmly entrenched as an organizational priority. Yet, only 17% of executives say they've spent more than a few days on cyber risk over the past year.

Source: 2019 Marsh-Microsoft Global Cyber Risk Perception survey

Data Privacy Laws & Regulations

Privacy risks typically are financial (fines & lawsuits) and reputational (bad press & negative perceptions). But new laws and regulations introduce risk around an individual's data rights and requests. Expect more people to exercise these rights.

Authentication

Technologies using AI and data analytics are emerging to support strategy and bolster defenses; however, many are still looking for ways to successfully integrate to improve processes and eliminate inefficiencies with authentication.

Cybersecurity Skills Gap

Lack of skilled / experienced cybersecurity personnel is a top concern. Not surprising is that 51% of cybersecurity professionals say their organization is at moderate or extreme risk due to cybersecurity staff shortage.

Source: (ISC)² Cybersecurity Workforce Study, 2019

Pandemic Impact

Remaining vigilant in a new environment.

Adopt a heightened state of cybersecurity preparedness and monitoring. Stay on the lookout for and defend against malicious activity.

COVID-19 outbreak re-introduces and re-prioritizes cyber risks

Global events such as Coronavirus (COVID-19) make all of us attractive targets for cybercriminals. Whether it's phishing emails, new targeted scams, or a change in business practices; these events can lead to challenging times. Here are a few risks that you should remain committed to at your credit union:

Scams

Coronavirus has been a windfall for fraudsters as they exploit the global thirst for knowledge on the virus. Fraudsters have launched Coronavirus-themed phishing attacks to deliver malware – typically credential-stealing banking Trojans. The phishing emails purport to be from the Centers for Disease Control and the World Health Organization. Fraudsters have also created fake websites to spread malware and have deployed scams involving federal stimulus package payments.

Bring Your Own Devices

Under a Bring Your Own Device (BYOD) program, organizations permit employees to connect their personal mobile devices (e.g. laptops, smartphones, and tablets) to the credit union's networks and systems to complete work-related duties. Credit unions must weigh the benefits and risks. Mobile devices are among the most vulnerable pieces of technology because they're easily exploited, can be quickly compromised by hackers, and open your credit union and confidential data to security risks.

Remote & Flexible Workplace Engagements

With a remote workforce, communication typically takes place in a decentralized environment. Privacy and security of member and credit union information should be a top priority. Additionally, remote workers should be provided with all the equipment needed to do their jobs. Your policy should state that equipment needed will be offered to remote workers. If you choose not to offer equipment to your remote employees, be sure that is clearly outlined. Consider these mitigation tips:

- Require anyone who uses their computer on public Wi-Fi to use a Virtual Private Network (VPN)
- Enable two-factor authentication, where available
- Protect data on personal computer by encrypted hard drives
- Require that every employee follow established data governance protocols

Network Access

Unforeseen circumstances can get in the way. And, as many of us are adjusting to remote / teleworking environment, it can present challenges and issues with access to the Internet and phone connections – most likely due to the increased remote work and stress it places on various networks due to overcrowding.

Check out the COVID-19 Outbreak Risk Overview for more info about these risks and mitigation tips.

Ransomware

Lock • Encrypt • Demand

A ransomware incident is one of the most disruptive and costly attacks your organization can suffer.

Data exposure driven by ransomware could be the next big wave

TRENDING

"Threat actors are definitely becoming more creative and more sophisticated.

Financial institutions need to be looking out for new techniques involving ransomware. It is one of the biggest concerns for both the loss frequency and severity.

In the past, they've threatened to release stolen data. However, now with the actual release, credit unions may need to treat these attacks more like data breaches. This means: notifying members, resetting passwords, and crafting messages to minimize your reputational impact."

Derek Laczniak, CIC
Director Cyber Liability, Partner
M3 Insurance

CUNA Mutual Group and M3 Insurance maintain a strategic relationship to manage brokered commercial products business and to share their expertise and insights with credit unions including the topic of cyber liability. M3 is one of the top 50 largest brokers of U.S. business.

Unfortunately, innovation and progress is on the upswing for the threat actor. For years, ransomware developers and affiliates have been telling victims that they must pay the ransom or else the stolen data and internal company secrets would be publicly released.

In fact, earlier in 2020, the FBI warned U.S. companies about ransomware attacks in which the perpetrator, sometimes posing as legitimate security vendors or a government agency, steals data and then encrypts it to further extort victims. The attackers warn victims that if payment is not made before the deadline, they will start publishing the stolen data.

"What we've been seeing in the underground is threat actors advertising their access to organizations, no matter the industry, and trying to find partners who have ransomware that they can deploy deep in those networks in a very customized fashion," reported Sandra Joyce, senior vice president of threat intelligence at FireEye.

Financial institutions – second most targeted industry in 2019 behind healthcare - need to be on the lookout. The fact that ransomware attackers can steal and encrypt data isn't a new phenomenon but the possibility that sensitive data might be revealed is potentially more damaging than short-term disruption caused by the malware.

Data could include member financial records, employee personal information, termination letters, salaries, and much more. This means organizations will have to treat these attacks like data breaches. Furthermore, if any third-party information is stolen, which is highly likely, then that requires further disclosure as well.

If ransomware developers do publish stolen documents or data, some experts think we could see lawsuits and public concern rise.

"With the increased focus on consumer data rights, more litigation could result from consumers who claim they have suffered damage as a result of these ransomware or cybersecurity attacks, suggests CUNA Mutual Group Senior Risk Consultant, Carlos Molina. Unfortunately, this will be a wait and see dilemma."

CUNA Mutual Group leverages the global experience of **Beazley Insurance** to monitor the latest cyber trends. By working on 775 ransomware incidents in 2019, Beazley has a unique vantage point.

Typical Ransomware Scenario

Initial compromise of your environment

- Fraudster targets your organization with a phishing campaign or through a poorly secured remote desktop protocol (RDP).
- Malware is successfully delivered to one of your unsuspecting users via a malicious attachment or web link in an email.

Malware is downloaded and installed

- The user opens the attachment and malware is unknowingly installed on the user's PC.
- The hackers undetectably explore your network looking for vulnerable systems and sensitive data.

Ransomware is deployed

- With access achieved, ransomware is spread across your network encrypting indiscriminately.
- The attackers have now encrypted and disrupted a material portion of your business.

Extortion

- The attackers demand a ransom – up to millions of dollars - for the decryption key.
- The attack can also become public knowledge which causes reputational damage.
- The regulator also wants to understand if there has been a mishandling of customer sensitive data.

Managing the Risk of Ransomware

It is critical to have a robust backup plan for all of your files. Some ransomware variants exploit backup systems as well. If your credit union does not use offsite or remote backup options, it's important that local backups are offline, regularly conducted, and not directly connected to systems where the ransomware can reach them. You should also follow these high-level suggestions:

- Train staff to recognize and report phishing campaigns
- Properly segment backups to prevent malware from spreading and infecting them
- Lock down Remote Desktop Protocol (RDP) ports
- Implement multi-factor authentication
- Ensure timely patching and anti-virus updates

Check out the Ransomware Risk Overview for more mitigation tips.

INQUIRING MINDS »»

What considerations should be made before paying a ransom?

The U.S. Government does not encourage paying a ransom to criminal actors. However, after systems and data have been compromised, your credit union must make the determination based on the impact of your organization and your members.

Remember that paying a ransom does not guarantee you will regain access to data or that data won't be publicized; in fact, some individuals or organizations were never provided with decryption keys after paying a ransom. In other scenarios, victims who paid the demand were targeted again and/or asked to pay more to get the promised decryption key.

Additional Resources

Beazley cyber insurance policyholders can access additional cybersecurity resources at www.beazleybreachsolutions.com (User ID / Password required).

Beazley resources include educational and loss control information relating to compliance, applicable laws, safeguarding information, preparing to respond to breach incidents and best practices.

Mobile Devices

The New Battleground.

The bad guys understand that there is a massive blind spot around mobile apps and are targeting mobile devices and apps because they present a path of low resistance.

Consumers aren't the only individuals adapting to the mobile-first world

The number of security incidents involving mobile devices has increased over the years. In today's tech-infused world, where almost everyone has a mobile device, privacy and data security are becoming increasingly prevalent issues. Ultimately, the compromise of a mobile device by a fraudster can be just as great of a risk as a desktop compromise of your member data, intellectual property and core systems of your credit union.

Many factors are making mobile devices more popular for fraudsters and a greater risk for corporate networks:

- Mobile malware
- Infected / malicious applications
- Out-of-date operating systems and unpatched apps
- Mobile phone scams
- Lost or stolen device
- Unsecured Wi-Fi and network threats

42 percent

of financial organizations experienced a security breach involving mobile devices during the past year.

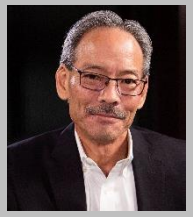
Source: 2019 Verizon Mobile Security Report

Mobile malware has grown by leaps and bounds over the years. In fact, mobile banking malware – often referred to as mobile banking Trojans - attacks boomed in 2019 with a 50% increase (Check Point Cyber Attack Trends: 2019 Mid-Year Report).

One of the key reasons for the sharp rise in mobile malware is the increased use of mobile banking applications. A few popular methods include infected applications; phishing / SMiShing attacks; malvertising; mobile ransomware; mobile banking Trojans; and SMS Malware.

Every device used to access credit union systems is yet another endpoint to secure, so one way of reducing risk is to provide access via a secure web application infrastructure with real-time vulnerability management. It's also essential for a credit union to have a solid BYOD program and security policy in place to help secure confidential data and protect credit union assets.

For more info on Mobile Devices & Technology Risks, access Emerging Risks Video Series and related resources.



Ken Otsuka
Senior Risk Consultant
CUNA Mutual Group

"The mobile app space has become a Wild, Wild West where anyone can build an app, and that can put everyone who downloads it at risk. This includes credit union employees. Many everyday apps are designed for simplicity and ordinary use without properly considering security."

Third-Party Relationships

Governing Third-Parties in the Data Chain.

Vendor due diligence and contract safeguards mean nothing if data privacy and security requirements are an after-thought.

Hackers look elsewhere for security vulnerabilities and points of entry

Decisions regarding strategic partnerships with third-party vendors are an increasingly important and complex issue for credit unions. Additionally, they do extend the risk of the exposure and misuse of your credit union's data. Consider yourself in a broader context — it's the entire ecosystem that you're a part of that matters.

It is key for credit union management to develop a thorough understanding of what each third-party relationship accomplishes for the credit union, and why the use of a third party is in your best interests.

Consider these vital steps for managing third-party 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 credit union and member data. Use some sort of vendor classification that substantiates and documents the rationale behind which third-parties are considered more critical than others.
- **Take necessary steps to understand your vendors' data security standards.** When applicable, contractually require adequate protection of member information and review appropriate security documents - request the vendor's Service Organization Control (SOC) 1 and 2 report - to ensure compliance. If vendors use subcontractors to handle sensitive data, determine if the subcontractors were properly vetted.
- **Know your vendors' cybersecurity strategies.** If your third-party vendors are entrusted with your credit union's member 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. You should know your vendors' policies on reporting data breaches.
- **Set expectations for your vendor relationships.** When making relationships with new third-party vendors, make cybersecurity a part of the vetting process and ongoing monitoring.
- **Understand your risk.** 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.

Carlos Molina
Senior Risk Consultant
CUNA Mutual Group

"Completing a **consumer data mapping exercise** can do a good job of providing a visual depiction of the data flow of personal information through applications, databases and third-parties. Unfortunately, not all vendors automatically merit a high level of confidence.

Ultimately, data maps provide the necessary foundation for the data analysis and compliance activities required by privacy laws."

C-suite Engagement & Governance

Cyberattacks are escalating...that's the motivation

The best cybersecurity infrastructure is unobtrusive, working quietly in the background as part of your fabric and culture.

Cybersecurity effectiveness requires a comprehensive C-suite approach

Cybersecurity governance is a dynamic risk area where credit unions need to adapt and adjust their priorities accordingly. 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 in their readiness and in establishing a culture of engagement.

CYBERSECURITY STRATEGY & GOALS

Establishing a quality cybersecurity governance program begins with risk management policies, a guiding strategy, and stated goals. The credit union's risk appetite should drive strategy and goals for the credit union's desired governance posture. Strategy should be articulated by senior leadership at a high-level and establish a roadmap to an enterprise-level policy.

A few key components to this strategy should be:

- Determining a risk appetite
- Identifying how cybersecurity risk relates to all critical business operations
- Establishing key performance indicators (KPIs) as well as key risk indicators (KRI)
- Identifying cybersecurity needs, objectives, and desired resources
- Call for an environment of continuous monitoring

SENIOR LEADERSHIP OVERSIGHT

Cybersecurity governance is an enterprise-wide concern. The focus and direction must come from the top to ensure that the process is successfully adopted. Without a "tone from the top" approach, the credit union's efforts will most likely fail.

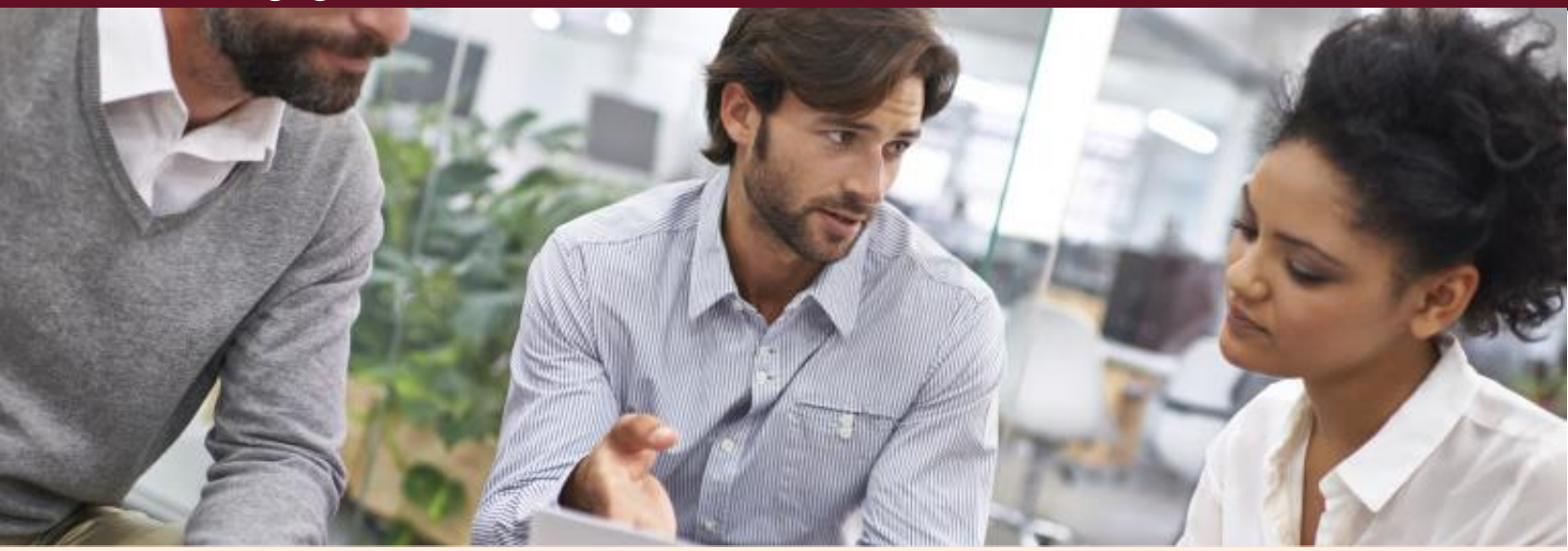
Senior leadership should be responsible for:

- Ensuring that established governance policy and objectives are compatible with the strategic direction
- Confirming governance policies and objectives are communicated to all relevant parties
- Require governance protocols be integrated into all credit unions processes and business lines
- Reinforce a commitment to continual improvement

INSIGHTS

*"Executives are more confident of organizations' ability to understand and assess cyber risk than of mitigating or responding to it. Just **one in five** respondents said they **are highly confident** in their organization's ability to manage, mitigate, respond, and recover from a cyber attack."*

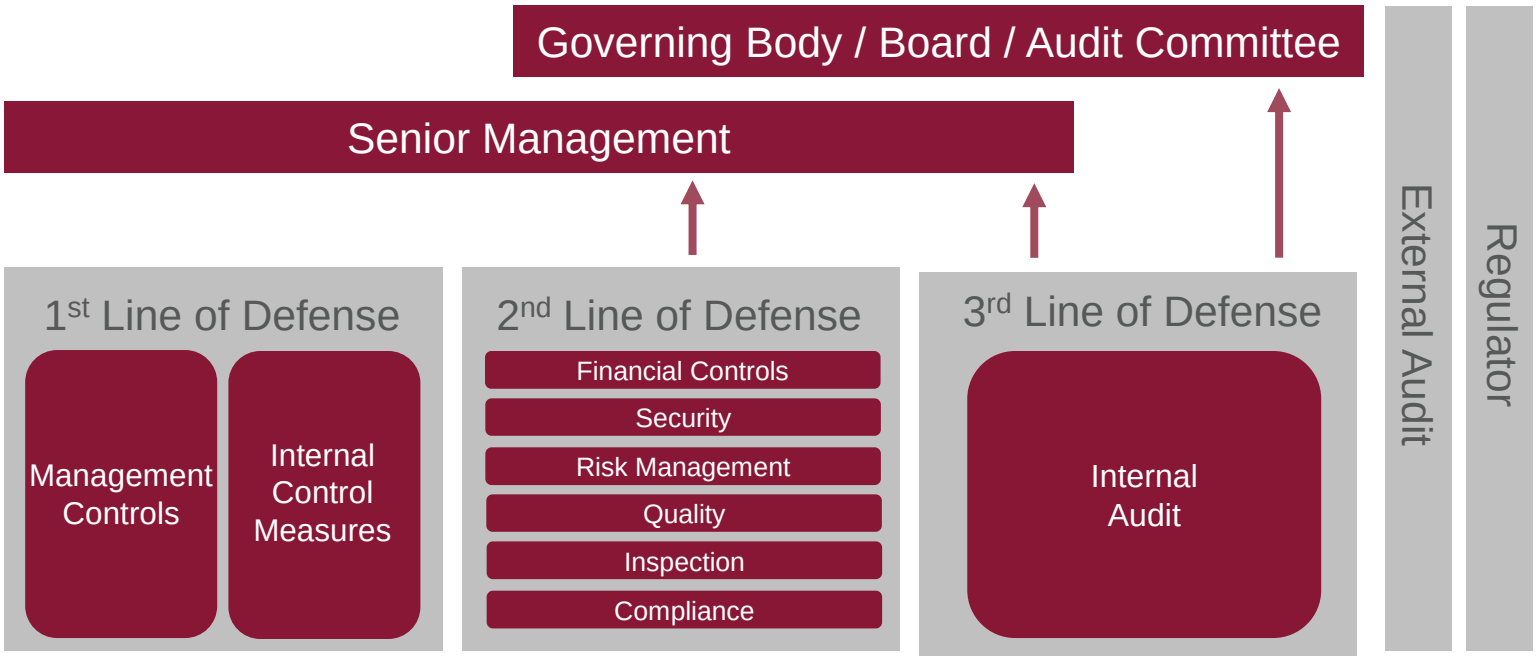
Source: Marsh-Microsoft Cyber Perception Survey, 2019



THREE LINES OF DEFENSE IN CYBER RISK MANAGEMENT AND CONTROL

Three lines of defense is **a best practice approach** to improve the effectiveness and efficiency of risk and control functions within organizations. This is often performed under an umbrella of senior management and some Board directors or a Board-level committee, such as the audit committee, cyber steering committee or a risk committee.

- The **first line of defense**, sometimes called management control, is tasked with managing cyber risks by executing various controls - handling certain risk events, updating key risk indicators (KRIs), and deploying / managing controls that affect people, processes and technology.
- The **second line of defense** brings risk, control, and compliance oversight functions responsible for ensuring that first line processes and controls exist and are operating effectively. The second line is often termed risk management but can also include compliance, legal, quality control, and financial control. The primary objective of this function is to monitor how management is doing in its handling of cyber risks by determining the extent that risks are actively monitored and appropriately managed.
- As the **third line of defense**, the internal audit activity provides senior management and the Board with independent and objective assurance on governance, risk management, and controls. This includes assessing the overall effectiveness of the activities performed by the first and second lines of defense in managing and mitigating cybersecurity threats and any associated risks.



Data Privacy Laws & Regs

Consumer expectations shifting faster than regs.

As data privacy and protection legislation grows, increased consumer focus around cyber risk will be a main driver.

Every organization needs to strengthen controls over access to sensitive data

With the growing wave of data privacy laws, such as GDPR and CCPA, organizations of all sizes are subject to compliance regulations that require you to implement and enforce access policies and have a way to document and prove compliance.

You should be able to answer these questions:

- Who has access to what?
- Who should have access to what?
- How is that access being used and how is it being controlled?

Next steps:

- Build and review holistic, risk-based privacy programs
  - Data mapping and inventories are first step
  - Align with other cross-functional programs – data governance, cybersecurity, third-party risk management, compliance
  - Follow or incorporate privacy framework developments (e.g., NIST)
- Educate and learn from your privacy stakeholders – IT, marketing, operations, security, etc.
- Watch regulatory developments, data security litigation, and AG enforcement closely. Pay attention to other states' and federal proposals

With a broadening push to offer more proof of compliance to industry regulations and requirements, with clear ways for consumers to validate you are doing what you say you're going to do; it is critical to allocate time and resources to compliance efforts.

In fact, adhering to privacy laws should be a collaborative effort among Chief Information Officers, IT teams, operational leaders, legal / compliance teams, and the entire C-suite. Efforts must be made to understand the context of data collection, processing, classification and use.

SHIFTING REGULATORY FOCUS

Making it even more difficult is that all 50 states in the U.S. have their data security laws, paired with a patchwork of industry-specific regulations and regulatory bodies. Some states, such as New York, have also implemented policies that force companies to submit proof of compliance with regulations.

As data privacy and protection legislation continues to grow, increased regulation around cyber risk will be one of the main drivers of the cyber insurance market. Cyber risk policies and programs, incident response plans and more are already mandated by different governing bodies. In fact, cyber insurance could become a necessary mandate to meet regulation standards.

THE IMPORTANCE OF MANAGING DATA RISKS

Conceptually, many organizations are trying to ensure that the trust in their brand is maintained and extended because trust is a fundamental part of relationships – especially credit unions. If your credit union acts ethically and ensures that the data use is ethical, and you maintain accountability, then your credit union brand is trustworthy. Credit unions must do more to protect their members and by doing so, they can protect their own brand and reputation.

Authentication

Members and fraudsters prefer online channels.

Member authentication continues to challenge credit unions as fraudsters learn to exploit weak authentication methods.

More obstacles needed to minimize the cloak of authentication anonymity

The online channel has quickly become a valuable tool for credit unions in providing member convenience – like account opening, loan applications, and other banking transactions. However, this also provides fraudsters with another channel and one with more obscurity challenging credit unions to properly authenticate and verify members and potential members.

Data breaches have fueled the problem and has significantly increased the number of identity theft-related fraud losses. The uptick in Social Security number compromises, in addition to other personally identifiable information – names, addresses, and birth dates - from these breaches compounds the problem.

ID Theft-Related Fraud Trends

New Account Fraud

New account fraud losses are increasing through the online channel. Fraudsters who open accounts at credit unions typically use stolen identities. In addition, these fraudsters make fraudulent deposits of checks or ACH debits and withdraw the funds before the items are returned unpaid to the credit union.

Loan Fraud

Losses stemming from identity theft-related loan fraud tend to be more severe in dollar amount than the losses associated with new account fraud. Once a fraudster opens an account, usually through the online channel, they immediately apply for loans, including unsecured loans, credit cards, and vehicle loans. These losses are increasing as more credit unions accept loan applications through the online channel.

Call Center Fraud

Fraudsters frequently target the call center and often request changes to members' contact information (e.g., phone number, email address, etc.) which typically leads to other forms of fraud, such as requesting wire transfers through the call center.

Account Takeovers through Online Banking

Fraudsters use stolen identities to impersonate members by enrolling member accounts for online banking. Once enrolled, they change the member's contact info through online banking. Then, once logged into the account, fraudsters take advances against member line-of-credit loans, such as HELOCs; request wire transfers; use bill pay or the external transfer service to transfer funds out of the member's account; use the external transfer service to initiate ACH debits to pull funds from external accounts for deposit to the member's account and then transfer the funds out of the member's account before the ACH debit entries are returned; or view canceled checks, including HELOC checks, to manufacture counterfeit checks.

Cyber Skills Gap

Real challenges, worrisome implications.
Cybersecurity talent is hard to recruit and retain for every organization. Without the right people (skilled and experienced) and right tools, this problem will continue to grow.

Cybersecurity is about people too… not simply processes and technology

Common Cybersecurity Challenges

64%
Changes / advances in technology

60%
Changes in types of threats

52%
Too few security personnel

51%
Missing skills in existing cybersecurity team personnel

Source: ISACA, CMMI Institute, Infosecurity Group, State of Enterprise Risk Management 2020

The demand for cybersecurity professionals continues to exceed supply, even though security teams have to deal with more threats than ever. In the U.S., the cybersecurity workforce gap is nearly 500,000. By combining our U.S. cybersecurity workforce estimates and this gap data, the (ISC)^2 Workforce Study suggests that the cybersecurity workforce needs to grow by 62% in order to meet the demands of U.S. businesses today.

With as many as two in three organizations worldwide reporting a shortage of IT security staff, automated security tools such as online vulnerability management solutions are fast becoming essential to maintaining a good security posture. Modern products can allow even a small team to efficiently secure multiple websites and web applications, providing a technological solution to pressing recruitment problems.

A closer look at cybersecurity professionals

Cybersecurity professionals are likely to have a bachelor's degree—with a little more than one-third holding a master's or doctoral / post-doctoral degree. While most in the field get their degrees in computer and information sciences (40%), others get degrees that are not IT-focused, such as engineering (19%) and business (10%).

They are more than twice as likely to be male, meaning there is an under-tapped demographic in women available for recruiting if companies can position the role in a way that overcomes common stereotypes. In addition, these cyber professionals tend to be experienced and long-tenured where they work.

Addressing the skills and talent shortage

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

Invest in employee development. Look to the 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.

Growing a strong cybersecurity workforce with the appropriate staffing levels is challenging but not impossible

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.

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. Use and recruit consultants / contractors. Post to technology-specific online job boards. Go to technical school and community college job fairs. Try to find candidates through organizations that offer cybersecurity certificate programs.

"While most of those in cybersecurity (56%) intended to work in this field — and most plan to remain in it for the rest of their careers — few started in it: Just 42% of respondents' first jobs after education were in cybersecurity."

Source: (ISC)² Cybersecurity Workforce Study, 2019

Staffing Outside the Box

We are in the midst of a security staffing shortage that demands rethinking what is actually required to do the jobs we have available.

What are the high-value skills that are hard-to-develop, versus the skills that a dedicated employee can learn over a reasonable amount of time?

Source: Road Ahead: Cyber Security in 2020 and Beyond, FireEye

Helping to drive job satisfaction is that the demand for cybersecurity skills creates a predictable career path. That desire for a career is built around the need for cybersecurity skills and the rapidly changing challenges that keep the job interesting. Many see that cybersecurity offers job security and is continuously evolving.

Limiting your candidate pool to people who have only worked in the financial sector will only compound the cybersecurity shortage. Instead of focusing on banking experience, widen your criteria to include different industries. A talented cybersecurity candidate can learn the ins and outs of working at a credit union on the job or rotational assignments to address any gaps in knowledge.

Cybersecurity readiness has room for improvement

"More than 90% of organizations believe the cyber risk landscape will stay the same or worsen in 2020. However, the majority (51%) of organizations do not believe they are ready or would respond well to a cyber attack or breach event. Moreover, nearly 29% of organizations with cyber attack and breach response plans in place have not tested or updated them in the last 12 or more months."

Source: FireEye Cyber Trendscape Report - 2020

Cyber threats can't be brushed aside, due to the potentially significant financial and reputational damage they can inflict on an organization. New technologies, such as AI and machine learning, can help detect and classify malware or spot suspicious activity across the network; however, establishing guiding principles for a successful cybersecurity roadmap, promoting accountability, and training employees to safeguard your data is just as important.

Unfortunately, organizations often struggle with cybersecurity because the methods of attack constantly change introducing new vulnerabilities. Additionally, a lack of experience in seeing cybersecurity done well is a concern. Cyber risks are one of the best examples of the need for cross-functional thinking and planning to anticipate issues and tackle risk management problems throughout your credit union.

Risk & Compliance Solutions • 800.637.2676 • riskconsultant@cunamutual.com