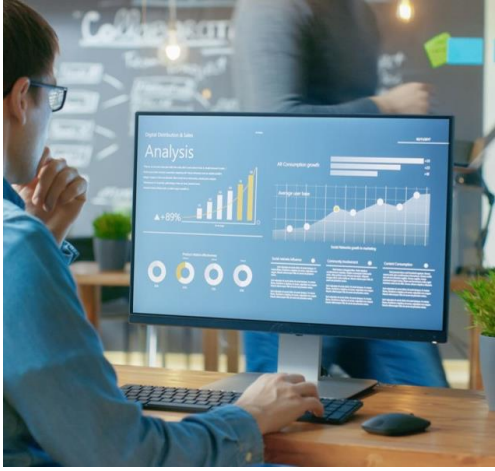
TruStage™

Cyber threats

Risk overview



Awareness of cyber threats has grown rapidly driven by the reliance on data, IT systems, and a number of high-profile incidents. Organizations also face a growing number of challenges including an increase in third party vendor incidents, rise of artificial intelligence (generative AI), the prospect of litigation, and a shortage of qualified talent to keep you cyber-secure.

Three main threats to data security

Cybersecurity strategies continue to quickly evolve as 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, cybersecurity threats can impact data security in 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 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 is one of the most dynamic risks for organizations to manage. Credit unions should commit to a thorough understanding of cyber threats, organization wide education on the current and next generation vulnerabilities and embrace key considerations for strengthening your risk posture across the entire organization.

$6.08 million

Average cost per breach within the financial industry.

Source: Cost of a Data Breach Report 2024, IBM Security

On the radar

- Ransomware
- Third-party relationships
- Data privacy laws & regulations
- Cybersecurity skills gap
- Artificial intelligence (AI)
- Phishing
- Business email compromise & fraudulent instruction
- DDoS Attacks
- Human element
- Geopolitical events
- Litigation

Ransomware

With the rise in ransomware attacks, so is the risk to all credit unions which often leaves organizations without data needed to operate. For years, ransomware developers and their criminal affiliates have demanded victims to pay the ransom or else the stolen data and internal company secrets would be publicly released.

> In fact, roughly one-thirds of all breaches involved ransomware or some other form of extortion technique, according to the 2024 Verizon Data Breach Report.

NCUA reports that in 2023, ransomware attacks and payments escalated in frequency, scope, and volume across all critical infrastructure sectors, including credit unions (Source: NCUA Cybersecurity Report 2024).

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have also warned U.S. companies about ransomware attacks and popular scenarios used 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.

Financial institutions continue to be popular targets for ransomware attacks and 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 held for ransom could include member financial records, employee personal information, termination letters, salaries, and much more. This means organizations should treat these attacks as data breaches. Furthermore, if any third-party information is stolen, which is highly likely, then that requires further disclosure as well.

Ransomware as a Service (RaaS) is another popular cybercrime business model in which a ransomware group sells its code to malware to other hackers who then use it to carry out their own ransomware attacks. This has made it easier for bad actors to carry out ransomware attacks.

> With the increased focus on consumer data rights, more litigation is quickly becoming a significant risk to credit unions resulting from consumers who claim they have suffered damage as a result of ransomware or cybersecurity attacks.

Paying ransom

Despite the threats, pressure, and stress from ransomware attacks, the FBI and other U.S. Government Agencies do 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 will not be publicized, has not been copied or duplicated; in fact, some individuals and organizations were never provided with decryption keys or return of all data 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.

Typical ransomware scenarios

Initial compromise of your environment

Remote Access Security

- Microsoft RDP and Remote Desktop Gateway (RDG) can be used to provide remote access to computers and networks.

Phishing/Spear Phishing

- Fraudster or threat actor targets an individual within your organization with a phishing campaign.
- Spear phishing targets a select group with something in common – e.g., work or bank at the same organization.
- Malware is successfully delivered to one of your unsuspecting users via a malicious attachment or web link in an email.

Malware is installed

- The user opens the attachment and malware is unknowingly installed on the user's PC. The threat actor now has a foothold in your environment.
- The hackers undetectably explore your network looking for vulnerable systems and sensitive data. This includes other users' PCs but also servers supporting critical applications and file stores.

Ransomware is deployed

- With access achieved, ransomware is spread throughout the network.
- Attackers have now encrypted and disrupted a material portion of your business. Some parts of your business are completely disrupted while other parts are partially disrupted.

Extortion is demanded

- 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.

Notification requirements

- Contact your insurance carrier immediately to report an incident or if you reasonably believe that you've experienced a reportable incident. Their breach coaches will assist you with the incident.
- The NCUA requires notification of incident within 72 hours. They also want to understand the incident including when it was first discovered, if there has been a mishandling of customer sensitive data, and investigation and remediation efforts.

Proactive prevention tips

It is critical to have a robust backup plan for all your files. Some ransomware variants exploit backup systems as well. If your credit union does not use offsite or remote backup options, it is important that local backups are offline, regularly conducted, and not directly connected to systems where the ransomware can reach them.

You should also consider:

- Training all staff to recognize and report phishing campaigns
- Properly segmenting backups to prevent malware from spreading and infecting them
- Locking down Remote Desktop Protocol (RDP) ports
- Implementing two-factor/multi-factor authentication
- Ensuring timely system, software and cloud patching and anti-virus updates
- Applying the principles of least privilege and network segmentation
- Vetting and monitoring third parties that have remote access to your network and other third-party connections

Third-party relationships

Governing third-parties in the data chain is critical. Vendor due diligence and contract safeguards mean nothing if third-party data privacy and security requirements are an afterthought .

Supply chain attacks make it easier for cyber attackers to circumvent security controls by creating avenues to sensitive resources through a target's third-party vendor. With third-parties often being connected to sensitive data, a single compromise could impact hundreds of companies and customers.

> 73% of total reported incidents since September 1, 2023, involved compromises within a third-party service provider.

Source: NCUA Cybersecurity Report 2024

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

It is critical, now more than ever, for credit union management to develop a thorough understanding of what each third-party relationship accomplishes for the credit union, the access to networks and types of information each vendor has, and why the use of a third party is in your best interests.

Managing third-party relationships

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 of framework for 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, practices, and controls**. 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 or deliver essential services, determine if the subcontractors were properly vetted and assess their risk profile along with due diligence review for your vendor's vendors (i.e. 4th parties).
- **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, including contractually requiring prompt notification of actual and suspected incidents within your vendor or their vendors, investigation, and cooperation. Keep in mind that reporting rules such as the NCUA 72 Hour requirements also extend to incidents with your third-party vendors.
- **Set expectations for your vendor relationships**. When entering into relationships with new third-party vendors, make cybersecurity a part of the vetting process and ongoing monitoring. Establishing expectations and obligations within the written contract is critical.
- **Understand your risk**. Establish processes to evaluate, re-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.

Data privacy laws & regulations

Consumer expectations are shifting faster than regulations. As data privacy and protection legislation grows, increased consumer focus around cyber risk will continue to be a main driver.

As of June 2024, 19 states have enacted privacy laws designed to increase protections for consumers' personal data, provide consumers with certain rights to control their personal data, and regulate businesses' use of consumers' personal data, including sensitive personal data.

Every organization needs to strengthen controls over access to sensitive data, especially consumer information.

With a broadening push to offer more proof of compliance to industry regulations and requirements, with clear ways for consumers to validate your organizations responsibility to protect and secure data, 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, risk management teams, internal audit, operations, and the entire C-suite. Efforts must be made to understand the context of data collection, processing, classification and use.

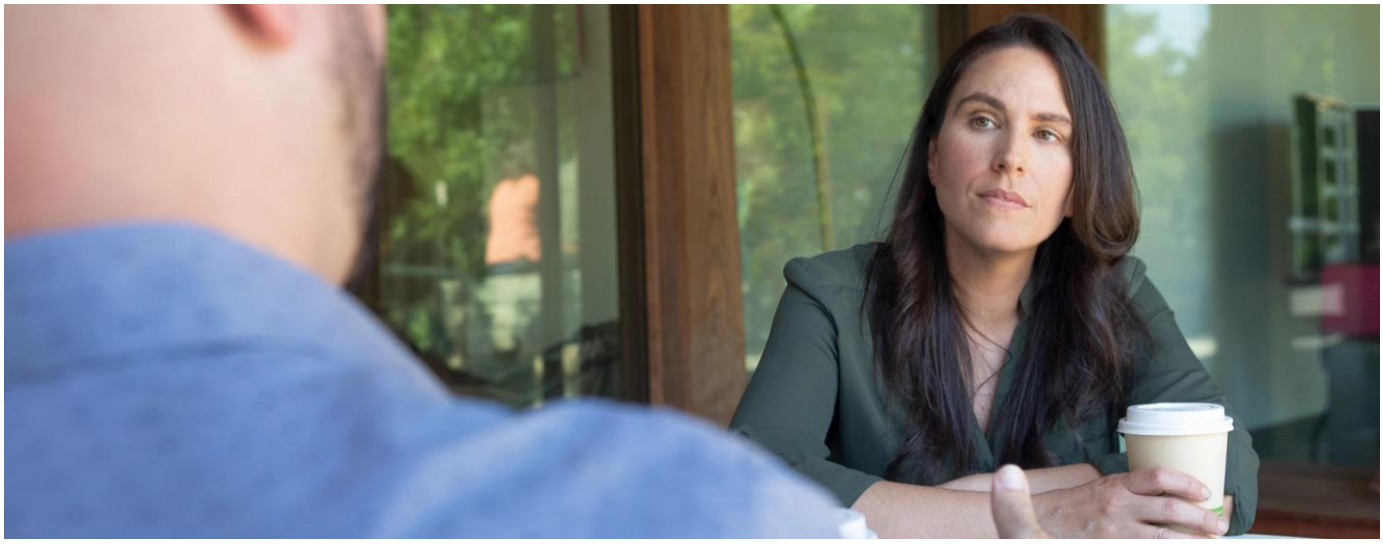
Shifting regulatory focus

Making it even more difficult is that all 50 states in the U.S. have their own data security laws with differing requirements, paired with a patchwork of industry specific regulations and regulatory bodies. Some states, such as New York and California, have also implemented policies that force companies to submit proof of compliance with regulations and document consent from consumers prior to handling such sensitive information.

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.

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. Credit unions must do more to protect their members and by doing so, they can protect their own brand and reputation.



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. The IT skills gap has widened since the pandemic.

Cybersecurity is about people too…not simply processes and technology.

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. Unfortunately, many IT professionals are being lured by other industries offering more flexible work arrangements and bigger salaries.

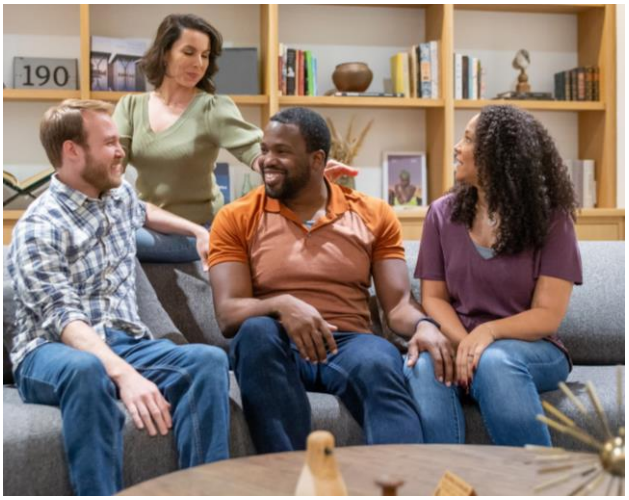
With as many as two in three organizations worldwide reporting a shortage of IT security staff, automated security tools such as **online vulnerability management solutions** are fast becoming essential to maintaining a good security posture. Modern products can allow even a small team to efficiently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

Many financial institutions have also turned to virtual information security officers, CIOs and CISOs rather than placing someone who lacks necessary skills.

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%).

SHRM predicts that by 2026, more than 90% of organizations worldwide will feel the pain of the IT skills crisis, amounting to approximately $5.5 trillion in losses caused by product delays, impaired competitiveness, and loss of business.

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.



Cyber skills gap

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.

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.

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.

AI risk considerations

With AI going mainstream and increasingly being used by cyber actors to create complex malware and advanced social engineering attacks, including phishing and spoofing, is making attacks more effective and harder to detect. It can be used to modify code to scale, quickly giving control to attackers. It can also be trained on data set of known vulnerabilities in rapid succession.

Cyber actors can also use AI to scan massive amounts of company data, summarizing it to identify employees, relationships, and assets, potentially leading to further social engineering attacks via user impersonation, blackmail, or coercion. Fraudsters are now deploying artificial intelligence to enhance fraudulent scam activity and create deepfakes to increase the effectiveness of their social engineering scams.

Using AI components like ChatGPT, fraudsters can create well-crafted phishing emails. Gone are the days when phishing emails were detected through misspellings and poor use of the English language.

However, users cannot simply prompt ChatGPT to turn out a phishing email because OpenAI has a set of rules that prohibits its use for nefarious purposes. Unfortunately, users are finding ways around these restrictions with the right prompts or inputs. Malicious actors share these specialized prompts, which are often referred to as "jailbreaks", in hacker forums.

Malicious actors have also taken to developing their own LLMs, such as WormGPT and FraudGPT, and advertise them for sale in hacker forums. WormGPT and FraudGPT are specifically designed for malicious activities, such as generating a phishing email, so they are devoid of any restrictions. In fact, WormGPT is frequently referred to as ChatGPT's evil cousin.

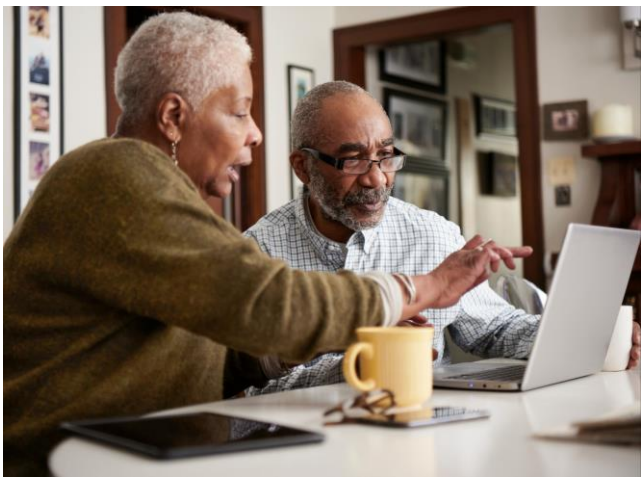
Phishing continues to grow and concern organizations. As a variant of social engineering, it is often a successful method of tricking users into divulging log-in credentials to gain access into an internal network

Scams against members

Fraudsters will also likely deploy deepfakes to enhance scams against members, particularly the romance scam. Fraudsters will look to lure more members in the romance scam using deepfake voices and videos to make the scam more convincing.

Scams against elderly members will also become more convincing using deepfake technology.

For example, an elderly member receives a call from someone pretending to be their grandchild (the perpetrator may or may not know the grandchild's name). The "grandchild" indicates they have been arrested, and they urgently need money to make bond. Circumstances may vary or be embellished such as they have unpaid tickets they must pay before being released, or they are calling the grandparent because they don't want their parents to know.



Business email compromise & fraudulent instruction

Generative AI has also enabled new, more sophisticated forms of digital impersonation. Fraudsters are using generative AI to create digitally altered images, video and audio of people saying and doing things they didn't say or do. Deepfakes will be a game-changer for fraudsters in social engineering scams, particularly the business email compromise (BEC) wire scam.

Business email compromise

Business email compromise (BEC) scams typically involve an executive level employee's email or phone number that has been compromised or spoofed through a phishing attack. The fraudsters create an email or text appearing to be sent from the executive to another individual within the organization requesting a payment – typically wire transfer, purchase of gift cards – divert payroll, or request employee W-2 information.

Fraudulent instruction

Like BEC, fraudulent instruction wire scams typically involve a fraudster looking to trick a member, credit union employee, or even a title company or closing agent. The scam is usually conducted via email with fraudulent instructions to wire funds to the fraudster at the last minute for a real estate transaction.

Impersonation scams often focus the request as "urgent" or "pay immediately" in hopes that the individual does not take time to scrutinize the request. Unlike traditional social engineering scams, the emails are hard to spot at quick glance and are rarely detected by spam filters.

In 2023, the FBI's Internet Crime Complaint Center received 21,489 BEC complaints, resulting in adjusted losses exceeding $2.9 billion.

Source: 2023 Internet Crime Report, FBI IC3

AI and deepfakes will take fraudulent instruction & BEC scams to new heights

The fraudsters only need a video sample of the person they want to impersonate to create a convincing video and/or audio with the use of generative AI. Video conference calls between employees of an organization is commonplace. A fraudster could use a deepfake video of a credit union's CEO in a video conference call with the CFO to request a large dollar wire. Alternately, a fraudster could create a deepfake of the CEO's voice and use it in a voice message or live voice call with the CFO.

Deepfake technology is rapidly evolving to the point where it may be impossible to detect a deepfake voice or video. Nevertheless, there may audio/visual clues suggesting a deepfake.

- Are there long, unnatural pauses in speech? This could be a sign that the fraudster creating the deepfake voice is using a text-to-speech model. It takes time for the fraudster to type the words to replicate.
- Be alert for slurring. The deepfake subject may slur certain words as the technology struggles to create words and phrases that the real subject did not say in their voice sample.
- Does the voice sound natural? Or is the voice monotone lacking in voice inflections that is a part of natural speech.
- Is there background noise? Is the voice crisp and clear or is there background noise like static?

For deepfake videos, pay particular attention to visual clues:

- Is there unnatural blinking by the subject, distorted facial features, or strange lighting or shadows?
- Do the subject's facial expressions, eye movements, head and body movements look natural? Do they match the context of the video?
- Pay attention to lip sync. Do the lip movements and spoken words align?

Distributed Denial of Services (DDoS) attacks

DDoS attacks continue to be a top concern for business organizations. These occur when a victim's website is overwhelmed with fake connection requests forcing it offline.

DDoS attacks are popular because the attack surprises drivers and compromises the banking IT infrastructure, customers' accounts, payment portals, and more.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

Impact is significant – can penetrate deeper for financial institution entities – cybercriminals can leverage the resulting chaos in two different ways:

- Additional cyber attack campaigns can be launched while the security teams are distracted by DDoS Attacks.
- Cybercriminals could offer to stop the DDoS attack if a ransom is paid – a strategy with the likelihood of success given the strict SLA agreements amongst financial institutions.

The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable. But since a number of causes — such a legitimate spike in traffic — can create similar performance issues, further investigation is usually required. Traffic analytics tools can help you spot some of these telltale signs of a DDoS attack.

- Suspicious amounts of traffic originating from a single IP address or IP range
- A flood of traffic from users who share a single behavioral profile, such as device type, geolocation, or web browser version
- An unexplained surge in requests to a single page or endpoint
- Odd traffic patterns such as spikes at odd hours of the day or patterns that appear to be unnatural (e.g. a spike every 10 minutes)

There are other, more specific signs of DDoS attack that can vary depending on the type of attack.

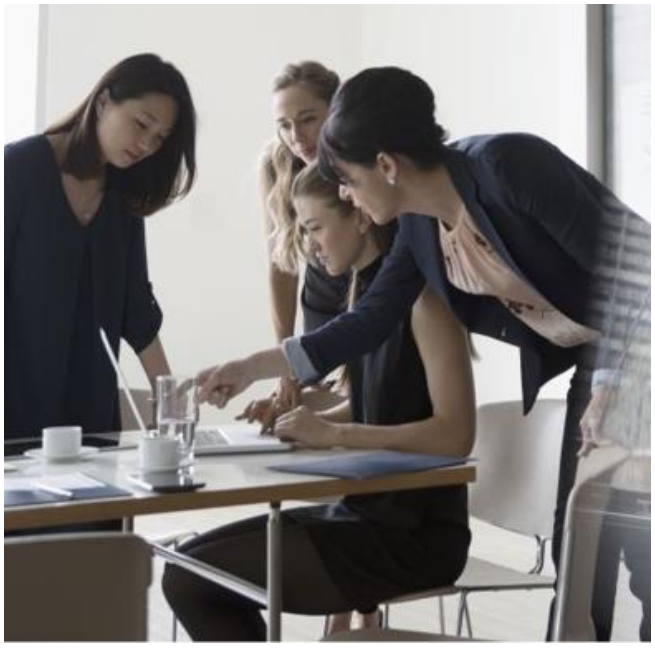
Human element

From poorly protected passwords to clicking on unsecure and damaging files and emails, there has been a significant growth in breaches involving human errors.

Many employees are unsure about their abilities to prevent an attack and lack knowledge about cybersecurity polices and practices for their organization, and unaware about the organization's process to report suspected cyber attacks even when their organization has a process in place.

Staying educated on cybersecurity risks and risk management strategies is the foundation of protecting your credit union's data.

You should 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.



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.

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.

Credit unions cannot expect employee engagement and accountability if they do not give them access to the right procedures, tools and knowledge. Cyber risks are one of the best examples of the need for cross-functional thinking to anticipate issues and tackle risk management problems

> 74% of breaches include the human element, including errors, stolen credentials and many forms of social engineering according to Verizon's 2024 Data Breach Investigations Report.

Other cyber threat considerations

Quantum computing

The rise of quantum computers, that harness quantum mechanics to produce far greater processing power could cause massive trouble, perhaps even decrypting the entire Internet.

Quantum computers will be able to break common encryption methods at an alarming speed. Attacks using a harvest-now, decrypt-later approach can enable adversaries to steal encrypted files and store them until more advanced quantum computers emerge. So, data with a long lifetime value, such as financial records will be of interest to bad actors.

Geopolitical events

Cyber actors have increased aggressive threats with aims of disruption or destruction of critical services to compromise critical American infrastructure, including financial institutions in the event of increased geopolitical tensions and/or military conflict with the United States.

The NCUA encourages credit unions of all sizes to adopt a heightened state of awareness and to proactively hunt threats to defend against this risk.

- Empower cybersecurity teams to make informed resourcing decisions to detect and defend against malicious cyber activity
- Develop comprehensive security plans and conducting regular tabletop exercises
- Secure your supply chain by establishing strong vendor risk management and monitoring vendor relationships
- Ensure your organization is aligned within leadership, IT, vendors, and business functions/units to facilitate a sound cybersecurity culture

Litigation

Many data breaches have spawned multi-plaintiff or class action lawsuits by customers whose PII was accessed by unauthorized third parties as a result of the breach.

Until recently, businesses faced modest litigation risk because most courts held that litigants lacked standing to sue in federal court, reasoning that plaintiffs had yet to suffer an injury, absent allegations that data exposure resulted in adverse consequences. The law in data breach cases is unsettled, and over the next years, courts will be forced to grapple with emerging issues.

Reports show that the number of data breach class action filings has soared in 2023. With stronger data protection under the law, an increase in cybercrime sophistication, and a heightened public awareness around data privacy due to high profile data breach cases, it is expected that the surge in class action will likely continue.

If your organization suspects, receives an indication of, or discovers any actual or potential incident, including incidents involving vendors, it is important to immediately contact your cyber insurance carrier. Providing prompt notice may aid with investigation, remediation of cyber risks, and notification requirements through the assistance of an experienced breach coach. Ensure key organizational stakeholders and IT personnel are aware of your cyber insurance policy and include it in your credit union's incident response and disaster recovery plans

Risk & Compliance Solutions
800.637.2676
riskconsultant@trustage.com