
*Southeast CUNA Management School 2022*

# Is Your Credit Union Ready for It?

**Lori J Collins**
**Purdue Federal Credit Union**
**West Lafayette, IN**
**lcollins@purduefed.com**

**Daniel Jordan**
**Acclaim Federal Credit Union**
**Greensboro, NC**
**daniel@acclaimfcu.org**

**Shari King**
**Shelby County Federal Credit Union**
**Memphis, TN**
**sking@shelbycountycu.com**

**Erika Perez**
**Lion's Share Federal Credit Union**
**Salisbury, NC**
**erika@lionsharecu.org**

# Table of Contents

# Introduction

Hello, fellow Credit Union Leaders. You are all here today because you have proven yourselves to not only be movers and shakers in the world of finance, but you are also dedicated to the movement of people helping people. Twenty-first century fact: wherever there are people, there is electronic data to go along with them.

As a Credit Union Leader, you are granted certain accesses and privileges to the data that matches the people you are helping. Now imagine that you are responsible for every single piece of data that flows through your credit union. Codes of all kinds, dates of all kinds, dollar amounts, addresses, rates, balances, every piece of it. You are responsible for where it comes from, where it goes, who touches it (employees, third party vendors, and examiners), who sees it, when they touch it, when they see it, what they can do with it when they see it, how they can get to it, and what happens with it when they're done with it.

In days past, that was the role of an Information Security Officer. But today, it is your role too. No matter what you do for your credit union, whether you are a loan originator, branch manager, credit counselor, accounting clerk, database administrator, whatever it is, it is your job to keep every piece of data that is available to you protected from harm, to keep it safe and secure on the credit union's network.

Now also imagine any of these scenarios at your credit union.

- An employee falls for a phishing email and now a malicious code has entered the credit union's network environment, locking and/or deleting data as it fingers its way through the system. The only way to get it back is to pay a ransom.
- An insider/third party with natural access to sensitive information has just abused the power of existing credentials and intentionally introduced malware to move data, prevent credit union access, and demand a ransom.
- Your credit union's network has just been inundated with a DDoS (Distributed Denial of Service) attack, overwhelming the ability to maintain itself. Now, the perpetrator overtakes your systems and wants money to stop the attack.
- An employee finds a planted USB device, labeled "Current Annual Salaries" and plugs it into the network to see what's on it. It was a bait tainted with malicious code. Now the network is locked down tight and there is no way to unlock it without paying the demand.
- A bad actor impersonating either a trusted vendor or IT staff member obtains an employee's credentials or access to the network closet. Once done, there is a ransom that has to be paid to get the credit union's data back within its own command.

Any of these scenarios can and do happen. It is how ransomware is integrated into systems and forces victimized businesses, like credit unions, to pay to get their own data back.

But fear not, for it is not all so bleak. There are things you, as a Credit Union Leader, can do to help keep data protected and secure, and to keep your credit union from a ransomware event. To help guide Credit Union Leaders everywhere, the following information was recorded from an interview with the Information Security Officer of a credit union.

- What is your main focus in your role as an ISO?
    - Answer: There are four areas that must be the top priority for every hour of every day. Those are **Awareness, Prevention, Detection, and Recovery.**
        - **Awareness** – what does a system user, at each and every unique level, need to look for and how can they be trained to recognize it.
        - **Prevention** – what are the security measures a credit union can put into place to keep an attacker from gaining access to the data.
        - **Detection** – how to set up security alerts in real time and how to respond to them before an event has the credit union under its control.
        - **Recovery** – how and when will the credit union be able to put a secure system back into operation.

      Additionally, keeping the kill-chain updated with standards to use to map against. This covers a workflow of standard operating procedures under a 'kill-chain' hierarchy in response to an attack.
- What do you specifically recommend for credit unions to do or for other ISOs to do?
    - Answer: There are several things. First, there is application whitelisting – a huge step and very instrumental in effectively keeping the network and the data safe from all kinds of harm.

      Also, be prepared ahead of time with a plan to recover. Keep the plan fresh and up to date, covering all types of scenarios and all applicable systems.

      Another important point is to test thoroughly and test often.

      Finally, if something is suspicious, don't try to fix it in live mode behind the scenes or in the activity. Shut it down first; then figure it out.
- Do you do any scenario testing then for all the types of cybersecurity, and if so, what kind do you do?
    - Answer: Yes, there is internal testing of course that should be done routinely, but external testing through a Red Team assessment is also recommended. Table-top exercises which involve play-acting an event can also open opportunities for improvement and help a credit union come up with plans for business continuity and disaster recovery, including from a cyberattack. Also, the Active Directory is one of the most important things to keep in the testing. The AD is the tool you will rely on to bring things back up, so if it is adversely affected by an attack, then it cannot be used in a restoration process.
- So then, what if the AD is adversely affected by the attack?
    - Answer: This is much more complicated and may mean that a full recovery by bringing systems "back up" is not possible or certainly not advisable. If the AD is gone, it has to be rebuilt from scratch.
- What is ransomware and what makes it different from other malware?
    - Answer: Ransomware is the specific use of a malware with the intent to capture and hold a company's data, preventing the company from accessing it in order to run 'business as usual'. The capture and holding of the data is normally achieved by encrypting the data or portions of the data and demanding payment to unencrypt. A main difference between the two is that ransomware is the last part of the attack chain, as the malware has already been deployed into the company's network before the files are encrypted.

- If any credit union is ever hit with a ransom demand, would you recommend that the victimized credit union pay it or not?
    - Answer: That is what is meant by 'be prepared ahead of time with a plan'. Is there cyber-insurance, and even if there is, does the credit union want to use it in that particular instance? The point is, an organization should never wait until in the midst of an event to stop and think about what to do and how to do it, as in decide whether to pay the ransom or not pay it. Have a plan ahead of time for when you will pay or not pay and stick with it. Also, if not paying the ransom means an organization has to recover and/or rebuild everything, then there should be an executable plan ready in advance for that too.
- Which is the right way to go, and how do you know?
    - Answer: It depends on the event, the data, the demand, and most importantly the ability or inability to recover. That is why organizations like credit unions have to run scenarios and be both prepared and capable of seeing their plans through.
- How does an ISO stay prepared and alert for attacks?
    - Answer: Education. Not just for me as an ISO or my IT staff, but full-on cybersecurity education for everyone. An educated employee is the best asset and protection an organization could ever have.
- What keeps an ISO awake at night?
    - Answer: A person can't possibly know what he doesn't know, and that is scary, because there is a lot of stuff to know. Also, critical patches can be hard to keep up with, and if there are any deployments that are late in coming from a trusted vendor, it could come back to haunt the ISO and the organization rather than the vendor.
- What helps an ISO sleep at night?
    - Answer: Knowing that the application whitelisting is working, knowing there is a good team in the organization, and knowing that the backups are performed and completed in more than one media type, meaning there is more than one potential way to recover from an event.

As you can see, every employee plays a role in information security, and while many ISOs feel a ransomware attack is inevitable for financial institutions in the current world environment, it also does not have to be the end of business for a credit union. Yes, you can help your credit union be **aware**, **prevent**, **detect**, and successfully **recover** from an attack.

# Research

Ransom demands have been part of extortion to pay the price for freedom or exchange of goods meaningful to the victim for centuries. With today's modern world and technologies, the new idea for a ransom demand is through ransomware, a type of malware that has been developed in sophisticated ways that have become untraceable back to an individual or a group of attackers.

Aids Trojan was the first cyberattack ransomware created by a Harvard evolutionary biologist, Dr. Joseph. It was first introduced by a floppy disk. A mail list was created where this floppy disk would be sent with the name *AIDS Information Introductory Diskette*. When recipients of this disk would insert it into their computers, it would then release the Trojan virus on their

system denying access to their c: drive files and forcing them to renew their expired license and pay $189.00 by sending it to an address in Panama. In today's world, no floppy disk nor a mailing list is needed. This all can be done by a simple email known as a phishing email.

Emails and text messaging have become a huge part of our daily communication system. You can have hundreds of emails coming in and out of your credit unions, but it only takes one click to download malicious malware and compromise your credit union's cybersecurity system and breach sensitive data. Phishing emails are among the highest methods used by cybercriminals because they can easily be disguised as coming from a legitimate source or organization. There are three types of phishing emails that are used to trick victims into opening and downloading any link or attachment or simply provide sensitive information.

1. **Spear Phishing emails** – these types of emails are the vast majority that are used to this day in the attempt to gather any information as possible online by the targeted individual or company.
2. **Clone Phishing emails** – an email will resemble a legitimate email previously received with similar wording or information making its victim trust it and click on any links.
3. **Whaling emails** – senior executives are the common victims in this group. Whaling emails will contain legal content addressed specifically to them such as filing a complaint within the company, or any legal actions against the company.

Social media requests, compromised credit card alerts, or invalid login credentials are examples of how cybercriminals trick their victims into providing personal or company data. One common fact when using phishing emails is the use of social engineering.

Costing billions of dollars in losses to businesses around the world, cybercriminals have made millions through ransomware since 2013, when one of the largest ransomware attacks occurred.

Ransomware became first well known in 2013 when there was an outbreak known as the CryptoLocker where several files and computer systems were affected. In September 2013, CryptoLocker took over close to 250,000 computers forcing its victims to pay in cryptocurrency. It was reported that $3 million were paid to its hackers.

Crypto Wall emerged from CryptoLocker in late 2013, and into 2014. This ransomware mimicked CryptoLocker and affected serval countries around the world. In the months of March through August of 2014, Crypto Wall infected nearly 650,000 systems and encrypted more than 5.25 billion files.

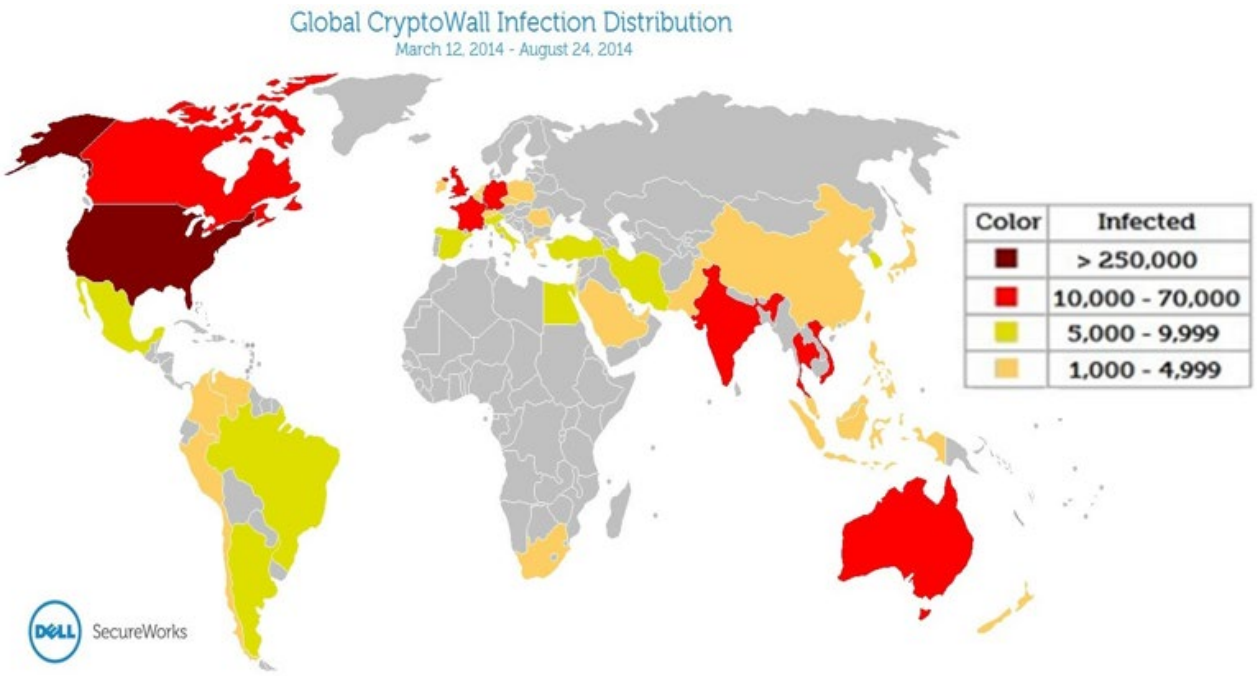



*Figure 1*: *Global distribution of CryptoWall infections between March 12 (approximate) and August 24, 2014. (Source: Dell SecureWorks)*

2021 was a big year for cybersecurity attacks and ransomware, as identified in the table below. Five ransomware attacks were recorded just in that year alone, demonstrating the substantial increase in risk nations are facing worldwide.

| 1989 | 2013 | 2014 | 2015 | 2016 | 2017 | 2019 | 2020 | 2021 | 2021 | 2021 | 2021 | 2021 | 2021 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AIDS TROJAN / PC CYBORG | CRYPTOLOCKER | CYRPTOWALL | TELSACRYPT | LOCKY | WANNACRY | TREVELEX | UNIVERSITY OF CALIFORNIA | CWT | CAN FINANCIAL | BRENNTAG | COLONIAL PIPELINE | JBS | KASEYA |

*Figure 2: Timeline of Ransomware attacks that made the news*

Over the years, cybersecurity authorities have observed this increase in ransomware attacks and how sophisticated the attacks have become. The top targeted industry, found in research done by Trellix, was the banking and finance industry, followed by utilities and retailers. These three industries alone made up 58% of attacks based on the research conducted from July through September of 2021. Banking and finance made up 22%, utilities at 20%, and retailers at 16%. In reality, any industry can become a victim of ransomware. Cybercriminals will demand payment and know that majority of the time a payment will be settled.

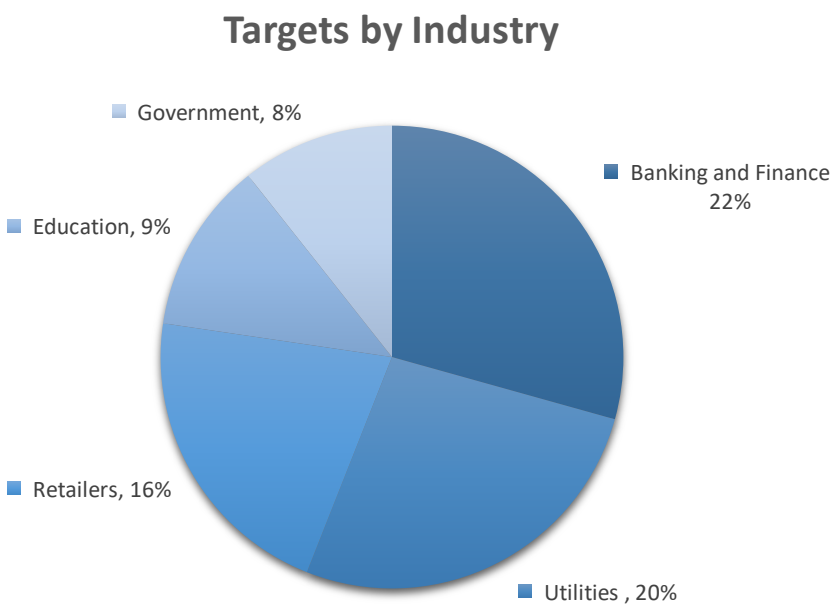



*Figure 3 Ransomware Targets by Industry*

Banking and finance industries are the top attraction simply because cybercriminals know this industry cannot operate while being shut down or while being denied services for a long period of time, forcing the ransomware to be paid. A Cyber Threat Intelligence Analyst, Stefano De Blasi, from Digital Shadows based out of San Francisco, CA, explained, "Cybercriminals often perceive organizations in the financial sector as wealthy and are thus incentivized to target them because of the potential of a high payout".

Due to Covid-19, new challenges were presented to the banking and financing industries in the past few years.

1. **Increase in ransomware attacks through Ransomware as a Service (RaaS)** – with this sophisticated form of licensed ransomware sold in the black market, cybercriminals are working together and getting a cut of the payout. With new forms of ransomware, it makes it harder for victims to fight against it.
2. **Digital banking – high risk** – part of growing with the digital world also comes the higher risk of open vulnerabilities, fraud, and compromised personal information. With online services, cashless operations, and convenient banking, financial institutions are being persuaded to develop digital applications or partner with third-party applications like Venmo, PayPal, or Stripe. While all these applications create convenience and benefits, it also increases the risk of cybercriminals accessing the institution's network. It also increases the vulnerabilities and malfunctions within data storing and transferring data. In 2019 Capital One's breach was the result of being a victim of such a vulnerability.
3. **Uninformed Employees** – phishing emails and downloaded links by employees continue to be one of the most effective ways to introduce ransomware into the network. While financial institutions invest every year in cybersecurity, employees need to be properly trained and up to date on new cyber threats.

4. **Cybersecurity understaffed** – with new risks and cyber threats, financial institutions, and other companies find it difficult to employ experts in cybersecurity and maintain their training in an up-to-date manner. The demand for cybersecurity is high and IT budgets are often not enough.

Several cybersecurity agencies such as the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigations (FBI) have all investigated and made several observations in just this past year, 2021. With ransomware being a high threat globally, these agencies are looking for similar trends and connections between the ransomware attacks and the industries targeted.

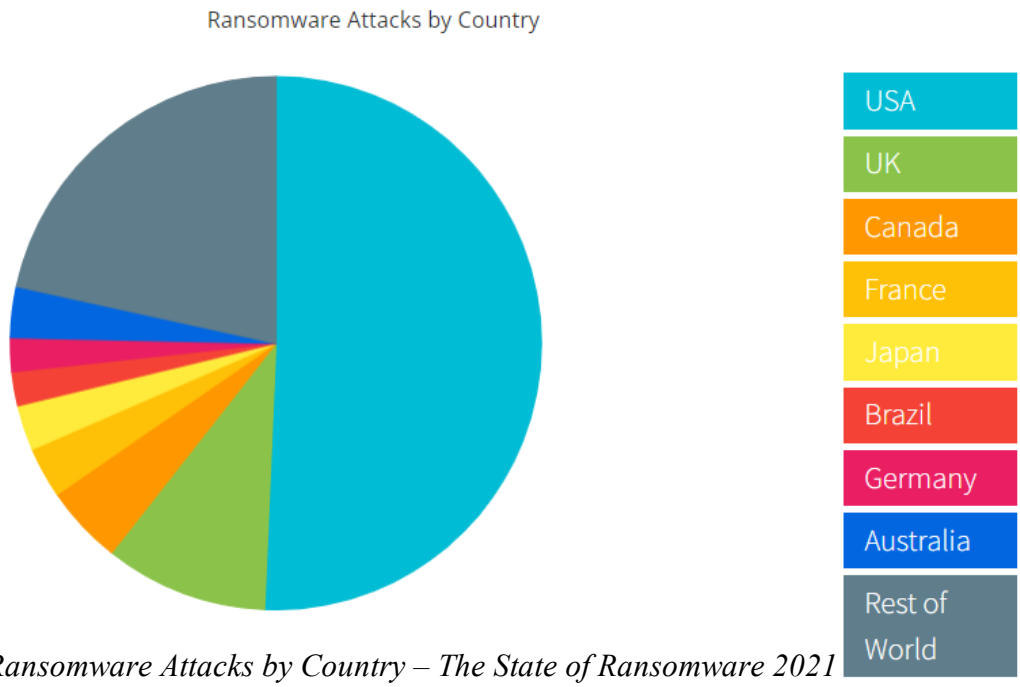



*Figure 4: Ransomware Attacks by Country – The State of Ransomware 2021*

Here are some of the common trends seen in ransomware attacks.

- **Phishing emails, access through system's vulnerability or stolen Remote Desktop Protocols (RDP)** – the majority of ransomware attacks occurring in 2021 started by one of these incidents due to the increase of working remotely and online classes in 2020.

- **Third-party services for payment negotiation** – this has become a well-established business within the black market. Cybercriminals will seek and employ an independent service to be a support system for their victims and negotiate the ransomware payment.

- **Ransomware on holidays and weekends** – it was found that cybercriminals use holidays and weekends when network security traffic is low and there are fewer IT support personnel monitoring their systems and offices are normally closed. This puts government and financial industries, including credit unions, at high risk. Several ransomware attacks that occurred in 2021 took place during weekends or major holidays, maximizing its impact and taking longer for victims to recover from it. Mother's Day, Memorial Day, and Fourth of

July are some of the major holidays on which ransomware attacks took place in the US in 2021.

- Mother's day / Colonial Pipeline – Darkside Ransomware
- Memorial Day / JBS – Sodinokibi/REvil Ransomware
- Fourth of July / Kaseya – Sodinokibi/REvil Ransomware

- **From the "big-game" to mid-sized victims** – after hitting hard the Colonial Pipeline Company, JBS Foods, and Kaseya, cybercriminals started shifting away from the "big-game" victims to mid-sized victims to reduce the potential risk of disruption from authorities. With credit unions being a cooperative, a ransomware attack on a credit union of any size can have a chain effect and spread easily on to other credit unions and even third-party vendors. Based on the table below provided by CUInsight, close to 90% of credit unions are considered within the mid to small-sized range and demonstrate the potential for the vast number of credit unions at risk for a potential ransomware attack.

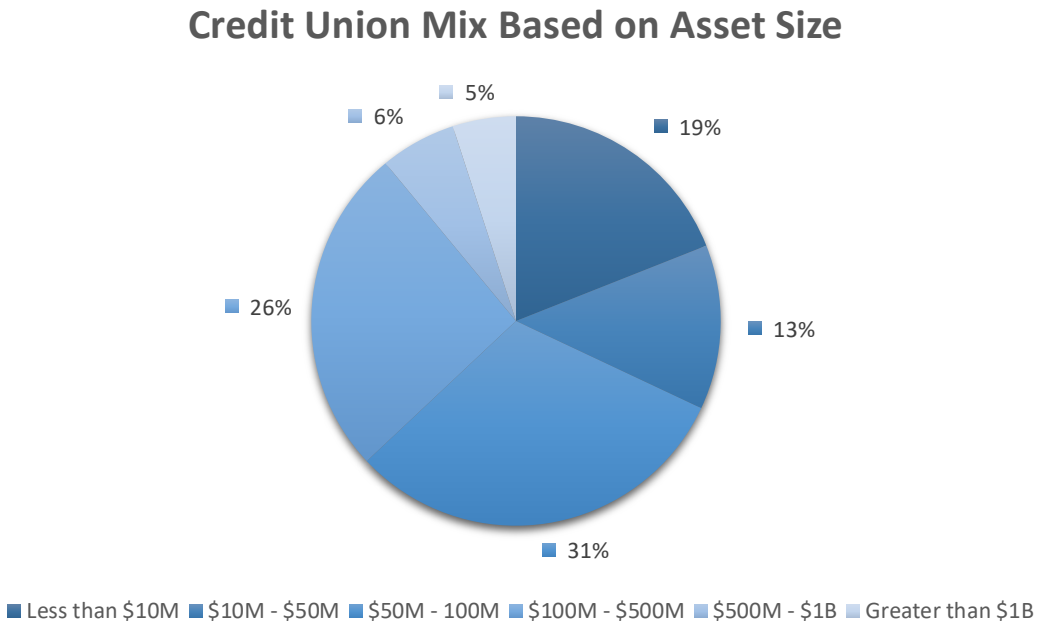


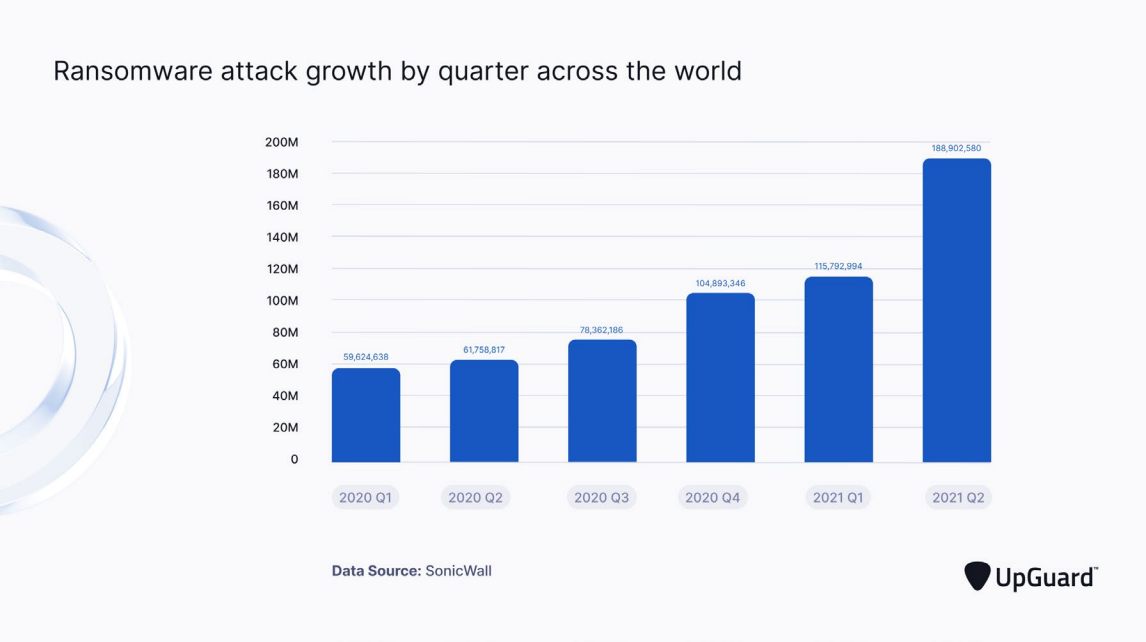

*Figure 5: CUInsight Credit Union Size*

Ransomware has become on high alert around the world and in every industry. With a 60% increase in 2020 and continuing growth, ransomware is putting organizations on their tippy toes and becoming the most dangerous threat. Due to the Covid-19 pandemic, the US has been on top for risk at a 158% increase in ransomware. Just in 2021, it was reported at 151% from the previous year during the same period.

So why has ransomware and cyberattacks become a global threat? The cybercriminal's goal is to seek payment with ransomware. They know ransomware will get paid at their demands and victims will be forced to pay in exchange for the release of a sophisticated decrypted key. Even though cybercriminals disappear once the ransomware demands have been met, not all victims

have been able to regain access to their data. However, cybercriminals must do their part as well and release such decrypted keys to keep their credibility and continue to get paid. This cycle is what makes ransomware an increasingly global growing threat.

The February 24, 2022, Russian military invasion and attack on Ukraine has caused global perils including those day-to-day normalcy activities that were secure and not a risk. America's fundamental infrastructure is now more than ever impacted by the threat of cyber-attacks that holds large and small institutions around the world at ransom. These acts are serious, a truth that must be dealt with, and one that is not going away on its own. Companies and individuals must fight back proactively and intentionally with software and technology measures unmatched against bullies who digitally attack our freedom, comfort and privacy in the workplace and at home.




Credit Unions like most financial institutions are in a direct pathway of ransomware attacks. The irony is that these staggering attacks are like severe weather storms. They are predicted to happen based on trends, but we just don't exactly know when and the where moment. To note, these costly malicious software and malware intrusions can prevent credit unions from accessing computer files, systems and networks. They are disruptive by nature and are permanently damaging in many cases to a financial institution. The long term impact is enormous and can cripple a company by impeding day to day operations or worst can drive a credit union out of business pending the amount demanded to be freed.

So, the question to credit union management is simple; how to make your credit union more secure? First, intentionality and or prevention is the initial measure to adopt as a front-line defense mechanism. The best practice is to avoid exposure to ransomware. This could include a

measure to routinely load and monitor anti-virus and anti-malware solutions that automatically update and run regular scans as a preventive step.

Communication, communication, and more communication to staff is a key benefactor of protecting and defending a credit union against Ransomware. Often personal data is stored on desktops. The Wall Street Journal recently wrote about how employees are surprised after being given notice that they have been laid-off that they cannot retrieve personal (and business related) information from their computers. The author notes that with advances in technology that often blur the boundaries between work and personal pursuits, many employees are hit hard when they cannot retrieve their personal contacts from their work devices or computer. All information stored must be wiped clean for security and data protection. Most workers know better than to store personal files on their office computer. But employees who spend much of their time at the office often treat the company PC as their personal gadget, filling it with music, photos, and personal contacts — even using the computer's calendar to track a child's sports schedule and other personal events. That makes it all the more distressing when an employee is separated from the credit union, he or she learns that their digital belongings are company property. Often times these policies will be provided to the employee when he or she first starts and signs the credit union's handbook.

Credit Union members expect and trust that their personal data and information is protected and stored at the highest level by spyware security. They also expect to be notified directly by the credit union versus the media if something goes wrong and their private profiles are compromised, stolen or frozen. A comprehensive communication strategy must coincide with a strong preventive strategy against ransomware. Urgent text messaging and email alert similar to an "Amber Alert" must be in the tool kit for credit unions when needed.

CUNA, NCUA, and other governing entities for national credit unions have tips and safeguards that are advantageous for credit unions. These measures are usually tested and have yielded the best safeguard against ransomware and other dangerous digital viruses that threatens credit unions.

Consultants and security companies with proven experience in the ransomware arena can be a certain resource to tap into for advice. These experts can measure your specific coverage and needs based on the various platforms and networks within the credit union. Usually, their technical recommendations are cost sufficient and seamless to deploy and maintain. Just like any other disaster recovery plan, a worst-case continuity plan should be thought out, documented and ready to execute as needed. A strong internal IT staff person who consistently and regularly double-check for attacks, stays on top of the latest trends and that blocks cyber bullies is important and worth every penny of a credit union's investment to keep this person nearby. Again, if the IT expertise does not exist internally to the leadership team, outsourcing is certainly an option to consider.

It's also likely that 2022 will be the year when IT organizations begin considering unified cloud-based platforms, such as artificial intelligence-based applications and services that exist in a cloud environment. As credit unions have shifted their IT infrastructures or adopted new ones, cyber-crime has ramped up to keep up. This is both a positive and negative as bad actors take advantage of this trend to increase ransomware attacks on companies who are changing infrastructure. The hybrid workforce requires a new approach to security and how credit unions should protect themselves from ransomware. Many experts believe and most would agree that

the hybrid workforce is here to stay, and it's an important one. If credit unions don't have a security policy that accommodates the needs of this unique group of workers, they are leaving themselves exposed to data breaches and other threats. Many organizations are discovering that a cloud-based architecture, especially one based on hybrid cloud technology, necessitates the adoption of a fresh approach.

Just as credit unions are securing and arming themselves, bad actors are moving faster than ever before to keep up. The manual processes of the past can no longer cope with this new attack time frame and vulnerabilities remain unaddressed until the damage is done. Malicious actors are now capitalizing on digital technology by employing automation and artificial intelligence in their attacks to offset defenses set up by credit unions. This has given them the power to rapidly construct more sophisticated multi-vector assaults that may be carried out at machine speeds.

Finally, a credit union defense against dangerous cyberattack is a unified collaboration to work together with other credit union and financial institutions. There are many practices that credit union boards and management teams can put in place to reinforce security for hybrid working. This needs to start with developing a cybersecurity policy and ensuring all employees and stakeholders are fully engaged. As part of this, it's essential to educate your employees on the importance of being aware of the threat, and how to counter it, including identifying and responding appropriately to phishing attempts, and physically protecting devices from theft. Continual training and reviews of employee cybersecurity awareness, tailored to the new reality of hybrid working, are key to making this happen. These are vehicles that affords opportunities to share threats, lessons, and defense strategies, not just within a single operation, but across industries as well. For credit unions to really be safe from ransomware they must take the threat seriously. It is time for all stakeholders to be actively involved in anticipating, preventing, and responding to potential ransomware and cyberattacks.

## Solutions and Practical Steps

As we have thoroughly laid out, the threat and consistency of ransomware occurrences are growing and increasing the pressure on financial institutions. In June 2021, the New York State Department of Financial Services (DFS) issued an industry letter to regulated companies it oversees, detailing controls the department expected the companies to have implemented to help prevent ransomware. To go along with our ISO interview in our introduction, we felt the following recommendations from the DFS would provide a list of steps and solutions your credit union can deploy to become more secure and ready for ransomware attacks. The cost of implementing the recommended security protocols can vary pending on credit union size and scope, more specifically the number of end users. While it can cause anxiety to ponder the annual cost of cybersecurity, the cost of being under secured is proving it can be exponentially more expensive.

1. **Email Filtering and Anti-Phishing Training –** Credit Unions should invest time in improving employee's awareness of their network security obligations and anti-phishing training. Required cybersecurity awareness training should include robust phishing training helping employees identify the most recent strategies of hackers. Credit Unions and/or a hired third party should also conduct periodic phishing exercises and test whether employees

will click on attachments and embedded links in fake emails. Should employees fail such a test, then the credit union should be prepared to provide corrective training and monitoring which will decrease the experienced risk. According to the Anti-Phishing Working Group (APWG), phishing attempts in the form of phishing sites and unique phishing emails increased exponentially over the course of 2020. The APWG also reported the Financial Institution industry as the most targeted industry at 4th Quarter end 2020. (APWG, 2021)


Emails should be filtered to block spam and malicious attachments and links from reaching users. According to Statista, a global provider of market and consumer data, spam messages accounted for 45.1 percent of email traffic in March 2021. (Joseph Johnson, 2021) While not all spam messages are malicious in nature, it is a commonly used method to deliver Trojans, spyware and ransomware. Not only will implementing an email filtering system keep your credit union safer from such attacks, but it also comes with the benefit of blocking emails that would otherwise have to be deleted by the end user, thus increasing employee efficiency.

2. **Patch Management –** Patch management is an essential process that deploys fixes to software and networks that have been identified by the developer. Deploying appropriate patches can keep bad actors from taking advantage of known security breaches that have been identified (known as the "Zero Day Award"), thus creating another line of defense against ransomware. Deploying patches also keeps systems updated and running smoothly for a better end user experience. Kevin Mitnick, convicted hacker and present day computer security consultant, said "security is always going to be a cat and mouse game because there'll be people out there that are hunting for the zero day award, you have people that don't have configuration management, don't have vulnerability management, don't have patch management". (Mitnick, n.d.)
3. **Multi-Factor Authentication ("MFA") –** MFA is a way to require more than one authentication factor to identify a user. That way, if one factor is compromised, there is

another layer of protection to prevent bad actors from gaining access to credit union data. "All logins to privileged accounts, whether remote or internal, should require MFA, as this is a highly effective way of blocking privilege escalation via password cracking" (New York State Department of Financial Services, 2021). When conducting business with third party vendors providing a service for the credit union, it's important to verify if they require or have the option of MFA for their product. It's possible you or your member could be using a product that has another layer of security to make data more secure.

4. **Disable RDP Access –** Credit Unions should disable Remote Desktop Protocol when applicable. "If, after assessing the risk, RDP access is deemed necessary, then access should be restricted to only approved (whitelisted) originating sources and require MFA as well as strong passwords. (New York State Department of Financial Services, 2021) In the Post-COVID-19 Era, remote employees will be more prevalent than in the past. It is important to assess and understand security related to RDP Access. "For the 2020 Unit 42 Incident Response and Data Breach Report, Unit 42 studied data from over 1,000 incidents and found in 50% of ransomware deployment cases, RDP was the initial attack vector". (Lightowler, 2021)

5. **Password Management –** Credit Unions should train employees about the risk of using easy passwords and require strong passwords across all platforms. "Privileged user accounts should require passwords of at least 16 characters and ban commonly used passwords". (New York State Department of Financial Services, 2021) Training credit union employees might be as simple as requiring them to use a passphrase as opposed to a password. Another option is to deploy a password manager software that generates strong differentiating passwords for each account you use. A password manager software can eliminate the frustration of having to remember so many passwords while increasing security. It is important to note that using a password manager software is not a guarantee of security, but coupled with MFA, can greatly increase the prevention of Ransomware.

6. **Privileged Access Management (PAM) –** Credit Unions "should implement the principle of least privileged access – each user or service account should be given the minimum level of access necessary to perform the job". (New York State Department of Financial Services, 2021) Implementing this process limits the amount of access a bad actor can gain when a single user is compromised. The PAM process can help identify weaknesses like multiple users accessing and knowing the same administrative password for a particular service.

7. **Monitoring and Response –** Credit Unions "must have a way to monitor their systems for intruders and respond to alerts of suspicious activity. Credit Unions should implement an Endpoint Detection and Response ("EDR") solution, which monitors for anomalous activity". (New York State Department of Financial Services, 2021) EDR is a platform that monitors computers on the network (endpoints) and not the network itself for suspicious activity which can include malware and various forms of cyberattacks. Using the function of application whitelisting, EDR can allow you control what applications and components are authorized to execute on the host and thus identify malware. EDR can isolate infected endpoints decreasing the odds of ransomware penetrating your system further, thus minimizing the magnitude of an attack.

8. **Tested and Segregated Backups –** It is important to maintain comprehensive and segregated data backups to ensure you're able to bring your systems back up with the most

up to date information. Testing your backups and scanning process will allow you to understand the amount of time you could be down in a ransomware situation. Keeping an additional back up offline is a way to increase your odds of hackers not infecting all data, thus making you more agile when a possible ransom request is made.

9. **Incident Response Plan –** To be fully ready for a real-life ransomware situation you must have a written plan for recovery. Thinking about what needs to happen in advance of an attack can be a great help in getting your systems back up and running. Once you have a written plan, you must test this plan thoroughly and on a regular basis. The testing should include the most senior management of the credit union, so the CEO is NOT testing the plan for the first time during a live ransomware incident. Addressing who is responsible for deciding if a ransom is paid should be documented ahead of time. Running test scenarios in which different levels of penetration are experienced can be helpful in establishing the credit unions tolerance/stance on paying a ransom request. According to the DFS, they and the FBI do NOT recommend paying ransoms. The reasoning, they explain is the payment of ransom "encourages and funds future ransomware attacks, and may also risk violating OFAC sanctions." (New York State Department of Financial Services, 2021) They also note the possibility of not being able to regain access to all your data and the likelihood of your data being resold even after payment. What is more, there has been increased occurrences of victimized organizations receiving subsequent attacks.

10. **Cyber-Insurance** – The DFS notes "Because of ransomware, loss ratios on cyber insurance increased from an average of 42% during 2015-2019 to 73% in 2020". The bottom line is premiums and the scope of coverage offered are being affected in this relatively new type of insurance market. Because of this rising cost, insurance providers must be more rigorous in assessing the cybersecurity of their customers and pricing insurance according to that risk. (New York State Department of Financial Services, 2021) By following the recommended steps from the DFS, a credit union can place itself in a better cost position with cybersecurity insurance providers. According to security.org, the current global market size for cyber insurance is at $7.8 billion with projections growing to $20 billion by 2025. This type of coverage could become normal for financial institutions. (security.org, 2022)

11. **Vulnerability/Red Team Assessments –** Credit Unions can bolster their defense against ransomware by establishing a "program to identify, assess, track, and remediate vulnerabilities on all enterprise assets within their infrastructure" (New York State Department of Financial Services, 2021). The Credit Union can perform such tests by itself or by hiring a team of professionals with fresh eyes to evaluate risk. The credit union should consider the staff experience and qualifications when making this choice, considering the importance of the function.

    When choosing outside help to test your defenses, two options you can consider are Penetration Testing and Red Teaming assessments. The two options are often used interchangeably but are different. Of the two, Red Teaming is a more in-depth testing. Penetration Testing will assess your cybersecurity to see where bad actors might infiltrate your system, how they would attack and the repercussions of the breach. Red Teaming will take it a step further and often apply more team members and resources to analyze your operation, like a bad actor would, and then proceed with a methodical approach to infiltrate your operations. "Cyber threats are constantly evolving, and threat agents are finding new

ways to manifest new security breaches. This dynamic clearly establishes that the threat agents are either exploiting a gap in the implementation of the enterprise's intended security baseline or taking advantage of the fact that the enterprise's intended security baseline itself is either outdated or ineffective". (Sehgal, 2018) Red Teaming your credit union on a regular basis will allow your cyber defense to stay up to date with the current threat tactics being used by bad actors. The process allows security events to be identified, patched and tested again to ensure the vulnerability has been neutralized.

# Conclusion

In conclusion, *are* you ready? Ask yourself if your credit union can handle a cyberattack this very second of this very day. What will your credit union do?

A successful cyberattack with a ransom demand will occur someday and it may be sooner than you are prepared for or can effectively handle. When it does occur, your credit union will need to be prepared to pay a potential ransom or recreate its data. Can it effectively and sufficiently do either one of those things at a moment's notice?

If you are ready and have a network that is regularly and successfully tested against a hacking event, if you have the ability to restore your network, data and Active Directory, have adequate cyber insurance, and have staff trained well in recognizing cyber threats, then you are in a good position.

But if any of those elements are lacking, you will need to heed the suggestions offered here and steer your credit union in a direction to successfully combat cyber terrorists.

Do your part by referring to the foundational elements discussed earlier.

1. Be **Aware** of Potential Cybersecurity/Ransomware Attacks. You can accomplish this by training your staff, ensuring that the training is up to date and ongoing, and by constantly communicating the importance of the role everyone plays in keeping the credit union safe.

2. **Prevent** an Attack. Prevention can be assisted through application whitelisting and other important tools such as locking down access rights and user privileges. Password management and multi-factor authentication procedures as well as remote access protocols are excellent measures every credit union should enforce.

3. **Detect** an Attack. Part of the IT environment in your credit union should include the ability to scan for anomalous and suspicious activity. The scanning should run continuous with the operations of the credit union as part of everyday activity.

4. **Recover** from an Attack. Planning ahead is your most valuable tool for recovery. As discussed, you should prepare and know what resources are available for recovery from an attack and how you can and will deploy those resources based on the circumstances of the event. Successfully stored and current backups, the ability to get to the Active Directory, and the ability to fund the ransomware should all be part of the inventory of your recovery kit.

# References


(2019, October 2019). Retrieved 2022, from https://www.cfisa.com/educate-your-employees-what-ransomware-is-and-why-you-should-care-about-the-risks/

Adlumin, K. (2021, June 15). What's the 411? Cybersecurity's Latest Ransomware Nightmare. *CU Insight*.

APWG. (2021). *Phishing Activity Trends Report 4th Quarter 2020.* San Francisco: APWG.

Bhasin, M. D. (2007, April). Mitigating Cyber Threats to Banking Industry. *The Chartered Accountant*.

Dossett, J. (2021, November 15). Retrieved 2022, from CNet: https://www.cnet.com

Fernandez, Y. (2020, June 2). What's The Difference: Malware, Viruses, Worms, Trojans, Ransomware, etc. *Xataka Basics*.

Finger, D. (2021, October 4). *Think You Are Prepared for Ransomware? You're Probably Not.* Retrieved 2022, from CSO Online: https://www.csoonline.com

Ganti, V. (2021, July 20). DDOS Attack Trends for 2021 Q2. *The Cloudflare Blog*.

*Handbook: How to Manage The Impact of Hybrid Working on Cybersecurity.* (2022, February). Retrieved from Admin Control: https://www.admincontrol.com

Henriquez, M. (2021, September 20). *Banking Industry Sees 1318% Increase in Ransomware Attacks in 2021.* Retrieved from Security Magazine: https://www.securitymagazine.com

*Hybrid Workplaces Likely to Be The Norm.* (2021, September 9). Retrieved from Insights Goodbits: https://insignts.goodbits.ai

Joseph Johnson. (2021, 07 20). *Spam: share of global email traffic 2014-2021*. Retrieved from Statista.com: https://www.statista.com/statistics/420391/spam-email-traffic-share/

Ledesma, J. (2021, November 22). *Cybersecurity in Banking: Bank Hackers, Ransomware, and More.* Retrieved from Business Insights: https://businessinsights.bitdefender.com

Lightowler, K. (2021, July 8). *Diagnosing the Ransomware Deployment Protocal (RDP)*. Retrieved from Paloaltonetworks.com: https://www.paloaltonetworks.com/blog/2021/07/diagnosing-the-ransomware-deployment-protocol/

Mitnick, K. (n.d.). *BrainyQuote*. Retrieved from www.brainyquote.com: https://www.brainyquote.com/quotes/kevin_mitnick

*National Cyber Awareness System Alert: Trends Show Increased Globalized Threat of Ransomware.* (2022, February 10). Retrieved from CISA: https://www.cisa.gov

New York State Department of Finance. (2021, February 4th). *Cyber Insurance Risk Framework*. Retrieved from New York State Department of Financial Service: https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02

New York State Department of Financial Services. (2021). *Ransonware Guidance.* New York: New York State Departemnt of Financial Services.

Pajor, P. C. (2021, July 14, November 29, December 3). Information Security Officer. (L. J. Collins, Interviewer)

Palmer, D. (2022, January 31). *Ransomware: Over Half of Attacks Are Targeting These Three Industries.* Retrieved from ZD Net: https://www.zdnet.com

*Ransomware: The State of Ransomware 2021*. (2022, January 4). Retrieved 2022, from Blackfog: https://www.blackfog.com

security.org. (2022, March 16). *Cyber Insurance Statistics*. Retrieved from Security.org: https://www.security.org/insurance/cyber/statistics/

Sehgal, S. (2018, October 18). *Red Teaming For Cyber Security*. Retrieved from ISACA Journal: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/red-teaming-for-cybersecurity

*The Rise and Rise of Ransomware.* (2020, September 22). Retrieved from Financial Services Information Sharing and Analaysis Center (FS-ISAC): https://www.fsisac.com

Trellix, S. (2022 , January). *Advanced Threat Research Report*. Retrieved from Trellix: https://www.trellix.com

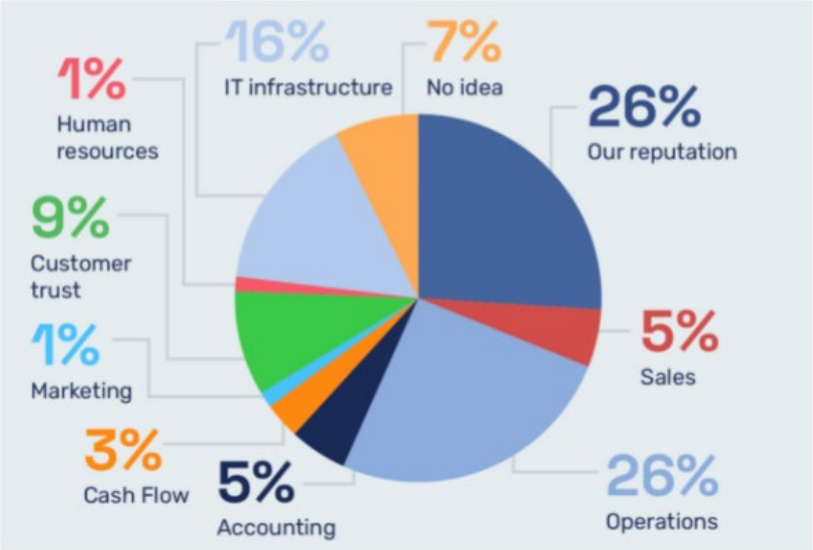
Zaller, A. (2016, May 13). *Employees Personal Data on Company Computers and Devices.* Retrieved from California Employment Law : https://www.californiaemployementlawreport.com

# Appendices

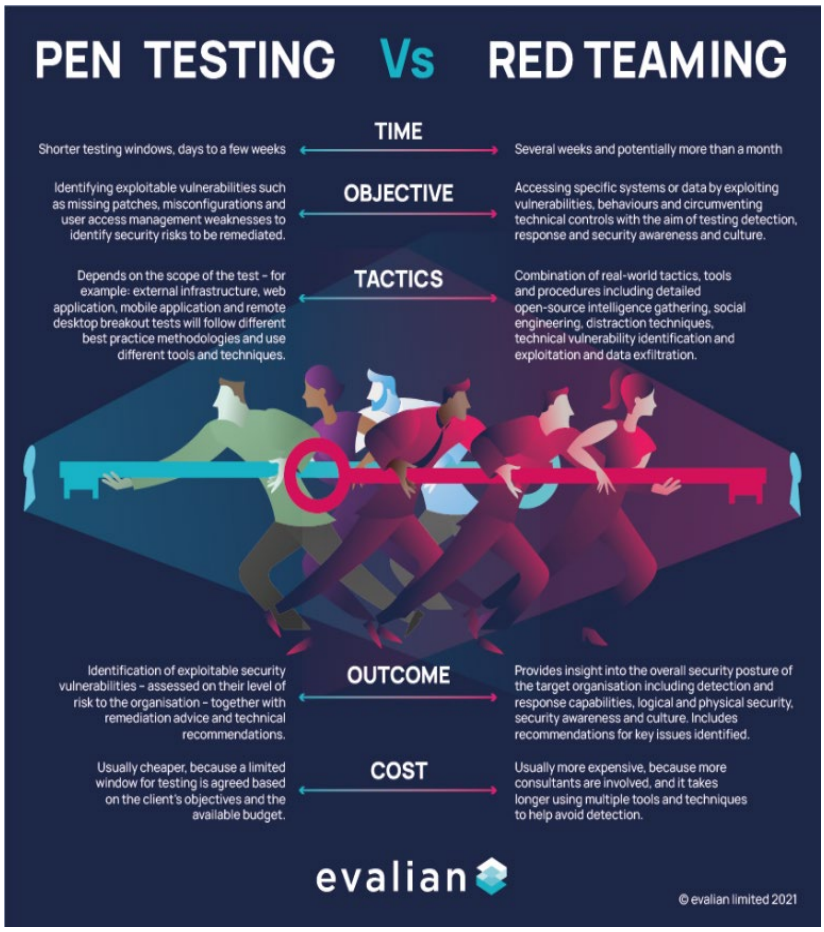
Ransomware 2022 Survey Results (Survey was taken by over 500 IT professionals)

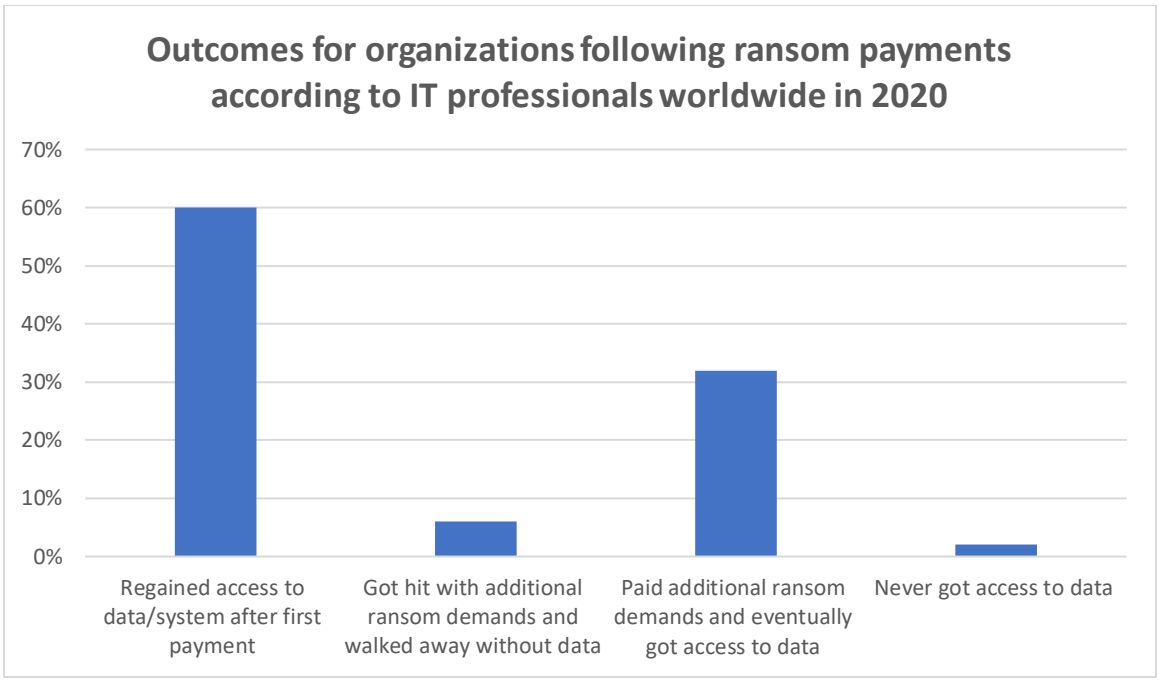
What areas within your organization would have a negative impact if there was a ransomware attack?

Respondents identified operations (26%) and their organization's reputation and customer trust (35%) as the top two areas that would be most negatively impacted by a ransomware attack. The exact cost of reputational damage can be hard to quantify, although BitDefender found that businesses can lose half their customer base after a data breach. And stalled operations will likely mean downtime, which can be extremely costly—in 2020, downtime cost American businesses $20.9 billion USD.

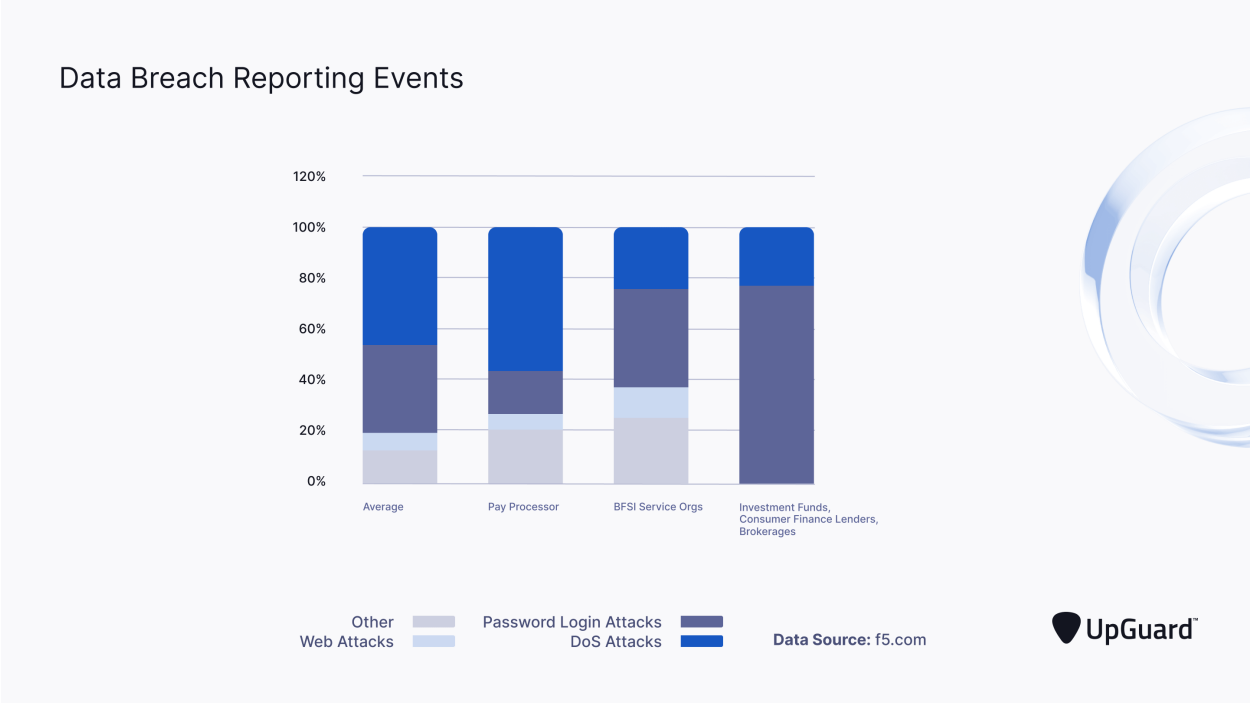


How can you remediate your credit union vulnerabilities?

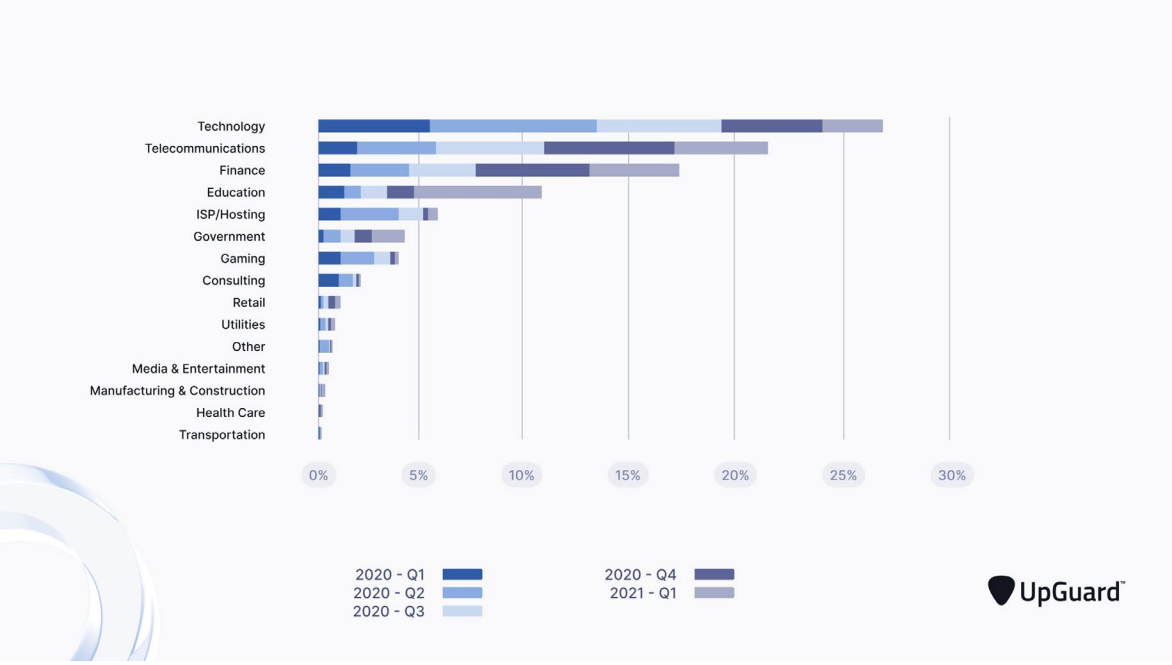





Password Login Attacks & DoS Attacks Were the Two Major Threats to Payment Processes in 2020



Finance is within the top three industries most targeted in DDoS attacks between 2020 and 2021.




(New York State Department of Finance, 2021)