PURESTORAGE®

WHITE PAPER

Winning the Ransomware War in Financial Services

Key steps for winning against cybercriminals.

Contents

Introduction

According to legend, Willie Sutton—one of the most prolific bank robbers of the 20th century—said he robbed banks "because that's where the money is." What does this notorious character have to do with today's ransomware attacks on financial services? A lot more than you might think.

The financial sector ("where the money is") is the single most important target for today's ransomware attackers, dwarfing all other industries in both frequency and number of attempts. That means cybercriminals, many of whom are actually well-organized businesses with a distinct profit motive, are logically going to focus on this high value target.

This white paper will separate fact from fiction regarding ransomware attacks and examine why financial-sector enterprises continue to be highly susceptible to breaches despite putting advanced security measures in place. We'll also explore how strategic thinking can mitigate damage before, during, and after any given ransomware attack, as well as how the right data storage solutions can make all the difference.

First, the Bad News

If you've done any research into cybersecurity, you've heard this before, but it's worth repeating: the challenge isn't *if* a ransomware attack will occur, but *when*. The hyperconnected, highly complex enterprise ecosystem (that increasingly encompasses remote workers using potentially unsecure home networks) makes the war on cybercriminals an ongoing series of endless battles. Taking a Titanic approach ("our infrastructure looks safe so it must be safe") is no longer feasible.

Here's why.

Like Willie Sutton robbing banks instead of grocery stores or gas stations, today's financial firms—trusted with our most sensitive personal and financial information—are highly desirable to cybercriminals. According to the New York Fed, such enterprises are subject to as many as three hundred times more cyberattacks per year than any other sector. In 2020 alone, phishing and ransomware attacks increased 520% in only four months.

A 2021 survey by Sophos, a British security firm, also presented some frightening statistics. More than one-third of financial services organizations surveyed were hit by ransomware in 2020. Of those, 51% said the cybercriminals succeeded in encrypting their data in the most significant attack. Over 40% of responding companies who were not attacked in 2020 fully expect to be victims in the near future.

The survey also uncovered that the average bill for rectifying a ransomware attack in the financial services sector—taking into consideration downtime, people time, device cost, network cost, lost opportunity, ransom paid, and similar factors—was $2.10 million. Keep in mind this is based on a survey of small- to medium-sized financial organizations. The average bill for larger enterprises is much higher. In fact, recent data reported by the Financial Crimes Enforcement Network (FinCEN) shows that in the first six months of 2021, financial institutions reported $590 million in ransomware-related transactions. If current trends hold, ransomware transactions in 2021 alone will exceed the previous 10 years combined.

Another survey by CSI showed 34% of bankers considered cybersecurity the greatest issue impacting their operations, far outranking traditional issues of meeting customer expectations and matching regulatory changes.

Money Isn't Everything

Surprisingly, money (the ransom) isn't always the only goal of an attack. In fact, there are currently more than 225 known exploit types that hackers successfully implement, with credential theft being a consistent favorite. Credentials are a form of currency on the dark web. Attackers that gain access to credentials can often sell them for more money (and less effort) than if they went through the more "dangerous" ransomware route. Many threat attackers want the fastest payout possible, so they prefer to simply buy credentials rather than go through the effort of carrying out an attack.

Also surprising is the nature of the attacks. Contrary to what the movies and television may portray, most attacks are not sophisticated in nature. They look for the easiest way in, such as software patches that were never updated or a vulnerable employee who could be tricked into revealing credentials. Automation, as will be discussed later, has accelerated this further. One malware program can do the work of a 1,000 Willie Suttons, with no human intervention even required. This is why there are so many attacks, so frequently.

Finding an Achilles' Heel

Bad actors know that financial institutions continually struggle to address cybersecurity, both across a complex enterprise and with legacy systems designed for another era. The data stored is especially sensitive compared with other industries, so much so that it often contains complete customer information (Social Security number, address, date of birth, and so on) that is a hacker's dream—one breach is all it takes.

Traditionally, storage of sensitive information in backups was viewed more as an insurance policy for worst-case scenarios, as well as a requirement for meeting regulatory obligations, since it was a laborious process to retrieve it. Today, backups are a primary target of ransomware attackers who understand that they are the last line of defense. Threat actors can readily gain "the keys to the kingdom" by using a multitude of attack vectors, including targeting a software or hardware vendor providing legitimate products and/or updates to the infrastructure—as well as phishing, exploiting security holes, and other attack methods.

But that's not the greatest challenge. Legacy storage infrastructures were built to secure a limited number of machines, such as within a single desk or department in siloed environments. That fact has not escaped today's savvy hackers. They know that when a ransomware attack occurs, restoring an entire business is a highly complex undertaking, and can take days, weeks, or even months to return systems to normal. And they definitely know such delays are not a viable option for any financial institution to undertake—the organizations need their operations up and running immediately. Especially since an attack can cascade globally beyond the financial institution itself, such as wreaking havoc on home loans, investment in new projects, or even entire financial markets. (Companies that are clients of the financial institution could go bankrupt and lay off workers due to delays, as one example.)

Therefore, "immediately" is where attackers make their money: pay the ransom or good luck explaining the situation to customers. In fact, cybercriminals often pressure their victims to make payment quickly by increasing ransom demands or threatening to release large caches of data. During an attack on CNA Financial, one of the largest U.S. insurers, attackers

informed the company that the cost for decryption was 999 bitcoins, or roughly $55 million at the time. The attackers subsequently raised the price without warning, stating, "Wasting time. The cost went up, 1099 BTC."

Dovetailing with this is an additional threat of going to the media, something that could potentially be the death knell for a well-respected bank or brokerage. Yet another potential threat that effectively rubs salt in the wound involves regulatory compliance and legal liabilities, including the inability to meet mission-critical recovery point objectives (RPOs) and recovery time objectives (RTOs).

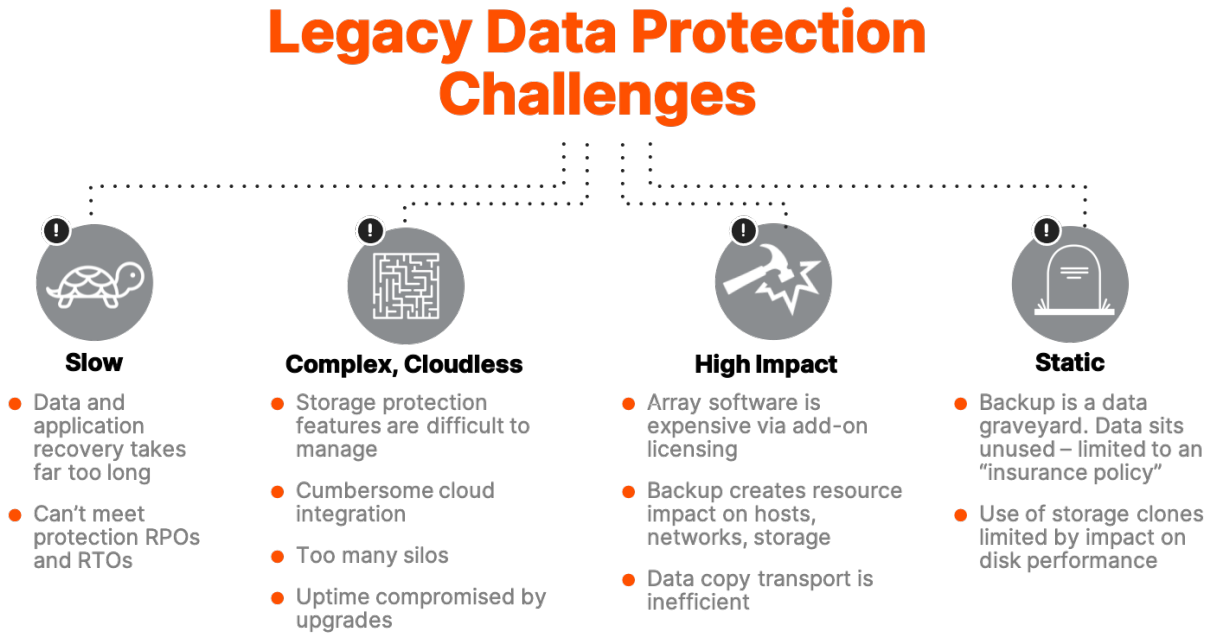

Figure 1: Legacy data protection challenges.

Now that the doom and gloom is out of the way, let's focus on gaining an understanding of what ransomware is and the modern solutions available to fight it.

A Ransomware Primer

One of the keys to protecting your financial institution from ransomware attacks is understanding the lifecycle of a ransomware attack, whether the intent is cyber espionage or simply extorting money. The lifecycle can be broken down into three simple stages: before, during, and after the attack. Of course, there will always be variations depending on the institution in question, the attacker's goals, and the amount of automation involved.

Before

During the before stage, an adversary performs reconnaissance on a target. The attacker launches a campaign, perhaps via email, to trick personnel within the financial institution into installing a small piece of malware that provides them undetected access. This clever ruse serves as a door into the organization's ecosystem and—contrary to what you might think—the individual who inadvertently installed the software is none the wiser that anything is wrong.

Once inside the security perimeter, the attacker will lurk or "dwell" in the environment and deploy a ransomware payload that will scan and map the network, as well as propagate to mapped/unmapped on-premises and cloud-based systems. In addition, the attacker will most likely prepare for the future as well. This involves creating additional backdoors on multiple systems and/or exfiltrating other sensitive files (those not required for the initial attack) for later subsequent attacks. Such actions increase the odds in the attacker's favor even if the initial breach is discovered.

During

Once the attacker determines that the discovery is complete, the encryption phase starts. The ransomware payload focuses on the backups first (for obvious reasons), which further cripples the financial institution's ability to defend itself. Typically, the most recent files are targeted first since they contain the most up-to-date information and involve active transactions. This ensures there is both money available (if that is the goal) and/or that threats will be relevant. For example, if hacked files from four years ago contain no account activity, it's possible the customer no longer exists and was simply not removed from the system—the threat is not as effective as with current customer information.

> **In the Real World:** At 5 am on Friday, December 13, 2019, the City of New Orleans director of operations for IT and innovation was alerted to suspicious server logins. It was the first clue that the city was experiencing a cyberattack. After shutting down hundreds of servers to mitigate damage, Pure Storage helped the IT team to quickly migrate data and replace its outdated storage infrastructure to get systems back online quickly and get citizens the access and services needed. The new storage lowers risk with fast backup, restore, and data snapshots. Learn more here.

After

This is where the real nightmare begins. Once the institution's targeted files are fully encrypted, a message is provided that outlines the demands. If the organization agrees to pay the ransom, an anonymous cryptocurrency account is provided. The promise is that once the ransom is paid, the attacker will provide the private keys required to decrypt/recover the files. Of course, this involves trusting the threat actor to deliver the keys, and many companies have found themselves paying the ransom but never able to restore all the files affected. And, as mentioned, a secondary attack may be invoked to extort more money—pay up or the data will be leaked to the media, posted to the public internet, sold on the dark web, or something else similarly nefarious.

But that may not be the end of it. If a financial institution does decide to pay a ransom to speed recovery or "hush things up," it potentially risks running afoul of sanctions regulations. According to the US Treasury Department's Office of Foreign Assets Control (OFAC) advisory on potential sanctions risks for facilitating ransomware payments, firms facilitating a ransomware payment may violate sanctions prohibitions, even if they have no reason to know that the transaction involved a sanctioned person or entity. Gives new meaning to Know Your Customer!

All this places organizations in an unwelcome position between a rock and a hard place. Even if the ransom is paid and the data is fully restored (a highly unlikely scenario to begin with), the financial organization could still have its operations impacted by OFAC regulations.

How Does a Ransomware Attack Happen?

There is a prevalent misconception that ransomware is just a malicious link that unleashes a virus. But as previously shown, the goal of the initial attack is to open a door (or as many doors as possible) to the financial institution's network ecosystem. And

while this paper outlines how attackers gain access—for example, tricking unsuspecting personnel—some hackers take the easy way out. They simply buy credentials on the dark web and gain access to an entire institution's ecosystem in seconds.

> **In the Real World:** In November 2021, a Congressional inquiry by the House Committee on Oversight and Reform looked into several multimillion-dollar ransomware attacks, including Colonial Pipeline, CNA Financial, and JBS Foods. In all three attacks, the cybercriminals appear to have accessed and infected the companies' environment via "small failures" in security systems. In the case of Colonial, the attack started with a single stolen password for an old user profile. In the case of JBS, the failure was an old network administrator account that had not been deactivated and had a weak password. CNA's attackers convinced a single employee to accept a fake web browser update from a commercial website.

That's why ransomware attacks represent some of the greatest threats in the history of financial institutions. The threat may be further exacerbated by the proliferation of public clouds and their connection with on-premises private ones. When Willie Sutton robbed a bank, he could only realize a finite amount of loot, even if he took every dollar. In the cloud era, it's like Sutton had unfettered access to endless tunnels that lead to other banks' vaults—and no one knew he was there.

While attackers may spend a lot of time (sometimes more than a year) exploring a system in secret without doing any damage, most attackers simply weigh the costs against the benefits—getting caught versus a bigger payout. They want to get in and get out quickly while maximizing the ransom. That's why the number one goal, even if they conducted a successful breach via paid-for credentials, is to attack directory services. They want to steal as many credentials as possible, especially "golden goose" ones that have priority access to sensitive files enterprise-wide.

In the example below, orange arrows indicate weak links of the chain (compromising credentials) where financial institutions are most vulnerable.

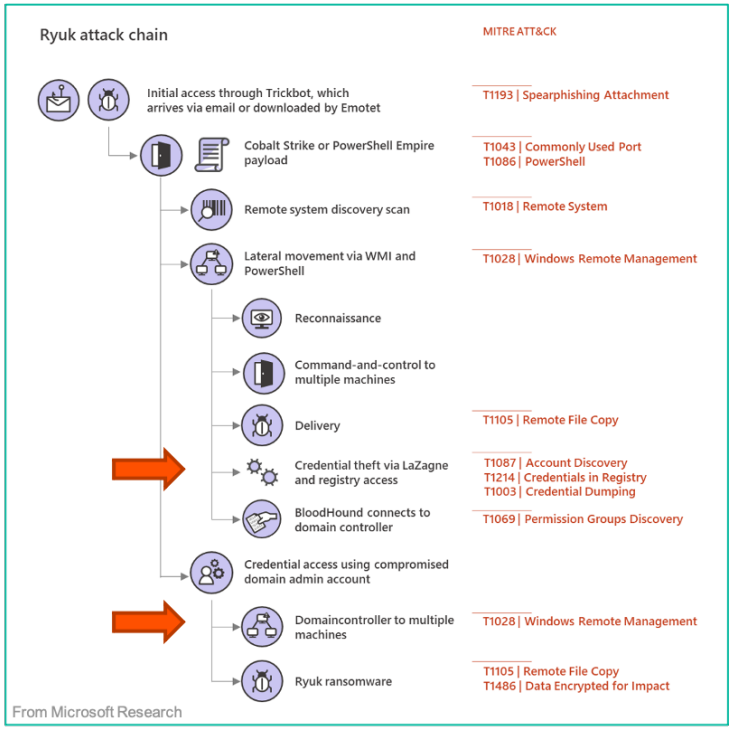

Figure 2: Ryuk attack chain.

What About "Undeletable" Backups?

Many companies think they are safe because they have read-only backups that cannot be deleted. Unfortunately, the sad fact is that with the right credentials an attacker can delete anything at any time. Imagine an expensive sports car with a top-of-the-line security system. The owner thinks the car is secure because of all the technology incorporated to protect it. But that system is irrelevant if a thief is able to obtain a copy of the keys (credentials), overriding any defenses—the car's security system thinks everything is okay, but the car is still stolen.

Ultimately, the attackers aren't using some special, *Mission Impossible*-style of attack. They're simply stealing credentials and logging into the financial institution's systems just like any administrator would.

> Did you know? During an attack, immutable Pure Storage® SafeMode™ snapshots are a great defense. Recovery snapshots cannot be deleted, modified, or encrypted even with admin credentials. It's peace of mind that every financial institution should have. Learn more here.

Key Points to Consider about Modern Attacks

In looking at ransomware attacks, it's important to understand that the attackers are businesspeople. Yes, they are techies, but they're also organized. They have built multibillion-dollar global businesses out of launching their attacks and getting financial institution victims to pay. That's why, like Willie Sutton, they spend time "casing the joint." They want to understand their victims inside and out, so they can optimize their potential gain in the most effective ways possible.

It's also why attacks are increasing in frequency, sophistication, and value to attacker—ransomware has proven to be a powerful tool to extort money from financial institutions. In fact, the value of the ransoms themselves has dramatically increased over the years, most likely due to both boisterous global economies and the advent of cloud infrastructures. There is an entire industry built around ransomware, including complete dark web ransomware ecosystems and even ransomware-as-a-service (RaaS) tools.

Attackers also have time on their side, and dwell times can extend to more than 400 days, depending on the industry, with the healthcare sector having the longest reported times. At the same time, ransomware attackers may leverage very advanced off-the-shelf or even open-source software that has reduced dwell times to as low as 12 days, with bigger payouts, thanks to automation. This level of sophistication also enables attackers to conduct a wide variety of concurrent attacks, including multiple attacks on the same institution, with little more effort than pushing a button or two. In fact, because so much ransomware has become commodified, there is an entire generation of less-tech-savvy "junior" attackers who can accomplish many of the same objectives as their sophisticated peers, yet with only a few hours of software training.

Reclaim Your Power

Despite the fact that the "boogeyman" is everywhere and can attack at any time, financial institutions have a lot of powerful defenses they can employ to ensure continuous operations, even after the most serious of breaches. It starts by gaining more and better visibility—finding indicators of compromise (IoCs) in the organization's ecosystem before an attack is launched.

When an event does occur, recovery is the number one mission-critical task at hand. Fast backups, lots of backups, and fast restore capabilities (plus something to restore from) are vital. After all, having backups in multiple locations doesn't mean much if every backup takes a long time to become fully functional. And don't forget that forensics must play an integral part in this

process, too. Simply recovering data is not enough, especially since crafty attackers could attach additional undetectable ransomware. Data must be cleansed before being released into the ecosystem, and that takes time.

The Security Lifecycle: Before, During, and After

This is where financial institutions can put ransomware lifecycle knowledge to good use. By mimicking (and matching) how such attacks evolve, teams can undertake specific security activities geared toward mitigating every phase of an event's lifecycle. This places the organization into a proactive mode rather than a reactive one, even if a breach does occur.

Before

No matter how great a ransomware prevention program is, it can be dead on arrival if there is not a consensus among those in charge. Therefore, it is vital that there is management- and board-level buy-in for any proposed strategy. In this way, all internal stakeholders are ensured their participation is completely sanctioned by the organization. Threat actors thrive when targeting financial institutions whose various personnel are siloed—especially when it comes to phishing/email scams—since such victims are typically less security-aware and/or have little incentive to interact with the larger security ecosystem. (They are not proactive, in other words.)

This "siloed complacency" is especially dangerous within the IT function. It is imperative that organizations focus on ongoing, consistent preventative maintenance and proper hygiene. Patch management is the key here. Unfortunately, these tasks just aren't sexy and are considered boring or mundane. IT resources, particularly security resources, naturally want to focus on new, fun, and exciting things. That means the less glamorous "unloved" items often get overlooked or deprioritized.

Ironically, guess who really loves the unloved? Attackers! They are always looking for the weakest links—especially unguarded ones created by technical debt and gaps. It is much like Willie Sutton looking for an unwatched entrance or weakened window frame.

Once the organization can get upper-level buy-in and emphasize how important unloved tasks are, it's time to get down to work. It starts by ensuring consistent logging across the entire environment, as well as implementing a comprehensive analytics platform to help identify signs of a threat actor. "Threat hunters," consisting of both human personnel and automated apps, should always be actively looking for (potential or real) breaches in the ecosystem, and then clean those compromised areas in a timely manner.

Augmenting these tasks must be all-inclusive security awareness training—with a focus on ransomware—that includes all credentialed stakeholders (employees, contractors, partners,and so on). Such training should also include communication procedures and channels to be employed if systems suddenly go offline due to an attack, especially if there is direct connection with a customer.

All of which are designed to mitigate what Willie Sutton knew was his most powerful secret weapon: people. Humans will always be the weakest link regardless of how secure every other component is.

During

During an attack the focus needs to be on identifying the nature of the attack and mobilizing incident response teams as quickly as possible. Often ransomware attacks occur in off hours, when offices are unattended, which is why adversaries will

frequently launch encryption campaigns in the middle of a weekend night while IT people sleep. By the time the attack is identified, the damage is done. Now it's mission critical to contain the fallout and start communicating as soon as possible.

It begins by activating instantaneous predefined lockdown procedures on which all relevant stakeholders have been trained. This is like a fire station where firefighters might be sleeping on a Saturday night, but they know immediately what to do once the alarm goes off. The first-response goal of security personnel is to identify the type of attack and the breadth of the breach: how much data is compromised, what systems are still working, and so on. Then the incident response team mobilizes and the various communication protocols are put in place. This is similar to firefighters getting information en-route regarding the nature of the fire, and communicating with associated response teams (ambulance, hazmat, police) for the best coordinated disaster mitigation possible.

> **Example:** In the event of a ransomware attack that compromises internal corporate communications, IT staff must have a plan for communicating with key stakeholders outside the ordinary channels, as well as defined levels of approval and the proper sequence of information flow.

After

After the attack, recovery and restoration efforts must spring into action. Every second of downtime costs money in one form or another, not to mention potential damage to the financial institution's reputation.

This stage involves prioritizing which systems are most vital based on which ones have been compromised and their "value" for immediate operations. Naturally, recovery efforts must begin offline in an isolated environment in case there is additional undetected ransomware attached. Forensic analysis must identify and clean ransomware infections, then methodically restore the systems into additional isolated recovery environments to ensure they are fully disinfected before being reintroduced into production. Finally, team members must communicate consistently and continually to relevant stakeholders in order to keep them up to date on the recovery efforts.

> **In the Real World**: In the Congressional inquiry mentioned above, Colonial told the Committee that the decryption key was used for some individual files, but not used more broadly for two reasons. First, the process of using the decryption key presented a risk of deleting legitimate files. Second, Colonial determined that using its back-up tapes was the better approach to bringing its systems back online because the tool provided by ransomware attacker DarkSide was too slow to be useful.

Modern Data Protection (and Solutions)

Mitigating the effects of a ransomware attack before, during, and after the attack revolves around two key metrics within an overarching recovery strategy: recovery point objective (RPO) and recovery time objective (RTO). RPO refers to how much data can the financial institution afford to lose, and RTO refers to how long can the organization afford to be down. This is where it is crucial to have management buy-in since there must be realistic answers to both. Simply saying everything must be recovered in the shortest time possible is the equivalent of an ostrich sticking its head in the sand. No matter how great an organization's security, there will inevitably be successful attacks. Therefore, designing a solution with the flexibility to offer different capabilities based on different needs and expectations is critical.

A tiered (layered) data protection architecture provides a modern methodology for protecting data across multiple geographies, while still making it highly accessible should the need arise. Depending on the service-level agreements (SLAs)

that the organization defines for RPO and RTO, multiple tiers of SafeMode snapshots can be established to support a long-term data protection strategy—complete with always available, high-speed recoverability.

> **Did you know?** Powered by Pure Storage FlashBlade® systems, Rapid Restore dramatically increases the speed of data restoration without the need to change backup software. It's a powerful advantage for meeting RTOs when large portions of data must be restored quickly. Learn more here.

In general, there are four well-defined layers that all relevant stakeholders must have a working knowledge of—and be able to intelligently communicate about—when the worst happens:

- **Layer 1**: Synchronous failover for instant recovery (RTO = 0) with no data loss.
- **Layer 2**: Near-instant recovery (RTO = minutes) with minimal data loss via asynchronous replication and/or localized snapshots.
- **Layer 3**: Recovery utilizing a secondary site with weeks of historical data—in a warm-standby mode—leveraging asynchronous replication and/or snapshots.
- **Layer 4**: Long-term data retention in a "bunker" mode. This typically consists of "one way in" and effective methodologies to recover historically aged data.

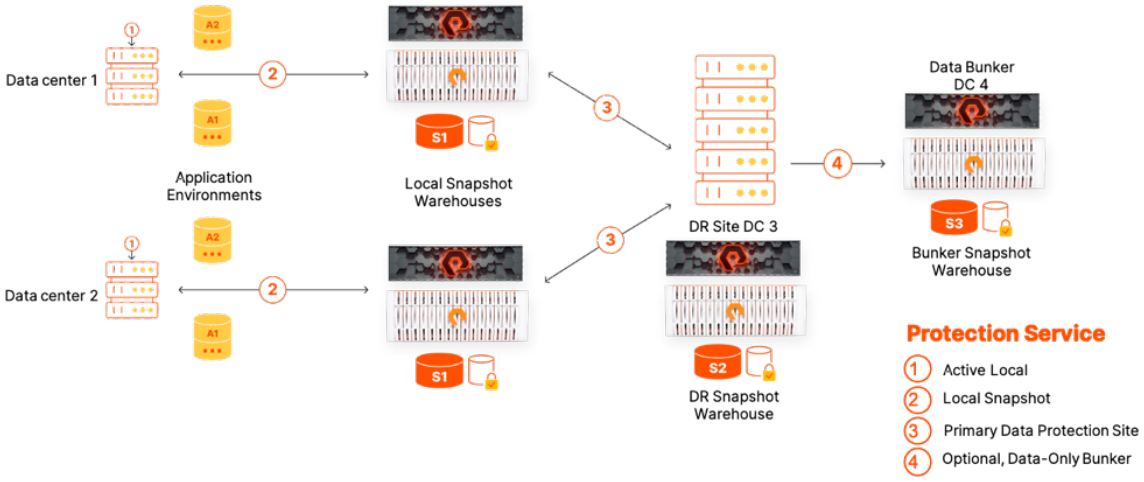

Figure 3: Example of how a tiered backup architecture works.

Conclusion

Wrapping up our ransomware discussion, it's important to reiterate that financial services continue to be one of the most targeted industries due to the sensitive data and monies being stored.

But money (the ransom) isn't always the immediate goal, and oftentimes credentials can be an even more valuable currency, especially since they can be repeatedly resold until the breach is detected. And while some attacks can take months to plan and execute, the reality is that the majority are based on breaching the weakest and most susceptible parts of the security ecosystem, typically via software patches and siloed legacy systems. Continuous and multi-pronged attacks are becoming more prevalent thanks to automation, and that technology has become so commonplace that even new-to-the-game threat actors can score big their first time out—they simply push a few buttons and deploy the malicious code.

> **Did you know? P**ure Evergreen™ storage and Pure as-a-Service™ enable financial institutions of all sizes to always have the latest hardware and software at their disposal, with no risky downtime.

Despite all the factors working against them, financial institutions can employ a variety of defenses—and proactive offenses—to mitigate any given attack before, during, and after the event.

Proper data protection planning and implementing the right infrastructure removes a lot of the pain. The tiered data protection architecture outlined above offers both resiliency and recoverability for any institution's RPO and RTO standards. But that's just one aspect. Clearly, action must be taken across the entire event lifecycle, including ensuring all the data is clean prior to redeployment. Speed of recovery is the most important factor and determines how much new investment will be required to make the company "whole." The more damage that is inflicted—such as ransomware bots lurking in the ecosystem for months,the more money will be required to rectify the situation.

Complementing these strategic and technological methods is the mission-critical need to change the psychology of the organization to a more security-aware stance.

At the end of the day, there really is little difference between one of the 20th century's most prolific bank robbers and today's geographically-dispersed threat actors. Their playbooks are the same: look for vulnerabilities, and then exploit those flaws to extract the biggest payday in the shortest time possible. At the center of every playbook strategy lies the greatest vulnerability of all: the human factor (or more specifically, human nature). Whether it was Willie Sutton choosing a bank at its most unguarded moment or a 21st century threat actor discovering an unloved (and unpatched) app, the security opening inadvertently created by personnel is something even the best protection and technology can't overcome.

This is why management buy-in, proper training and consistent non-siloed knowledge, predefined communication protocols, and other intangible safeguards are so important. To revisit the fire station scenario, it might seem that the firefighters are simply going about their day in a traditional manner, especially if they are sleeping at night. But once the alarm (an "attack") occurs, every member of the team knows exactly how to be proactive and mitigate the damage, including following strict communication protocols with external stakeholders.

No financial institution will ever be 100% safe from bad actors, and that's a sad reality. But by being highly proactive—both from a strategic technology perspective and a psychological one, organizations can significantly mitigate the initial damage of an attack, and then successfully recover in the fastest times possible.

What to Do Next?

- Get informed: Hear former black hat hacker Hector Monsegur discuss the essential steps to take before, during, and after a ransomware attack.
- Get your Ransomware Survival Kit.
- Check out how Pure Storage can protect your financial institution, today and tomorrow.
- Download the Hacker's Guide to Ransomware Mitigation and Recovery eBook.
- Dive deep with a Pure Storage ransomware solutions technical brief.
- Attend a (short) Pure Storage Ransomware Advisory Workshop.

About the Author

Diane Saucier is financial services director at Pure Storage, leading the solution marketing efforts for financial services, FinTech, and RegTech. She has held key roles with global financial institutions and technology vendors developing multi-asset class trading, risk, and compliance solutions. She is a founding board member and past president of global non-profit Women in Listed Derivatives (WILD) and is an advisory board member for the University of South Florida FinTech Program and John J. Lothian & Company, Inc. Diane holds a bachelor's degree from Northwestern University and a patent for a flexible system for electronic trading.

Pure Storage, Inc.
650 Castro Street, #400
Mountain View, CA 94041