The Ransomware Report

A Tale of Three Breaches

TABLE OF CONTENTS

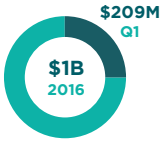
BLAST FROM THE PAST: RANSOMWARE OF YESTERYEAR

It's 1983, and Ronald Reagan is sitting down to watch the hit film *War Games*. Five days later, the President asked his secretaries of state, "Could a scenario like *War Games* ever happen?" One week later, General Vessey returned with the answer: "Mr. President, it is a lot worse than you think." Was this the first time that cyber security and privacy had surfaced in computer systems? Absolutely not. *Security and Privacy in Computer Systems* by Willis Ware was the first paper on the topic—written back in 1967. Since the beginning of networked computing, cyber security and privacy have been integral components. The uses and idea of cyber warfare were frequently discussed within government since 1967, but ransomware was not yet a household name like it is today. An example of how this began to change took place in 2007 when Idaho National Laboratory ran the Aurora test, which demonstrated how a cyber attack could destroy physical components of the electric grid. The experiment used a computer program to rapidly open and close a diesel generator's circuit breakers out of phase from the rest of the grid and cause it to explode. This vulnerability is referred to as the *Aurora Vulnerability*.

The Aurora test provided proof that cyber attackers could inflict physical damage using computer tools and increased the understanding of just how much impact cyber warfare could have. This was a pivotal moment, as critical infrastructure was at risk. Over time, cybercrime then shifted to the public sphere with cyber groups lining their sights on non-government attacks like online fraud, ransomware, malware, and phishing. Due to the meteoric rise of cybercrime over the last decade, the role that security and privacy now play in IT and our personal lives is huge. Strong security practices have gone from a nice to have, to an expected standard.

THE PROBLEM

While ransomware may come in many forms, it is ultimately about encrypting data that another person or company owns. This encryption may be done by another person or by an organization that then charges you to decrypt it. Essentially, your valuable data is being held ransom. With the complexity of current IT architecture and the practical impossibility of keeping all the components in the modern datacenter up to date with appropriate patches at all times, ransomware will not be slowing down any time soon. Ransomware has dominated headlines over the last few years as businesses were, and still are, targeted. 2017 alone has seen some huge headline attacks—WannaCry, Bad Rabbit, and NonPetya all targeted businesses to encrypt their data and charge a ransom. To give you an idea of ransomware's recent impact:



Q1 2016: $209 million in revenue with 2016 totaling $1 billion

56,000 infections per month

101 known ransomware families

Government estimates ranging past $10 billion in 2017

Delivery via a range of mechanisms from exploit kits, to email, and website links

What many are not aware of is the ecosystem that underpins these ransomware families. The *Cerber* ransomware family, for instance, accounted for 70 percent of all attacks this year up until #WannaCry and illustrated the increasing accessibility of "Ransomware-as-a-Service" or RaaS, now available to an audience beyond cyber criminal groups.

SO HOW DOES RAAS WORK?

RaaS leverages a franchise deployment model. In the IT world, this is very similar to the channel or the Value Added Reseller model. Instead of writing their own code, aspiring cybercriminals can purchase a RaaS kit with different price points, billing models, encryption methods, technical skill level requirements, and more. While early forms of ransomware were not overly sophisticated, the Cerber family exhibited an unprecedented amount of detail and sophistication. Cerber characteristics to know:

Flexible: an encrypted JSON file or other configuration options give the user the ability to change settings such as targeting certain file types, avoiding certain language packs or IP ranges, or performing environment checks to look for antivirus or related protection.

Adaptive: modern ransomware looks for almost all file types including VMs, databases, scripts, and email. It gains persistency in Windows and has fault or watcher processes to support persistence via respawning.

Detection: if Cerber detects it's being hunted, it will shut down and not run. UAC mode is completely bypassed.

Encryption: encrypts without having any internet connectivity, has 2048 bit RSA encryption keys in its payload, and encrypts your data with a high degree of entropy.

Reporting: sends statistics home via UDP including any environmental information available.

RaaS is one economic factor that has resulted in ransomware attacks exponentially increasing because it widened the pool of people who were able to commit such an attack. Another fiscal piece of the ransomware puzzle is the rise of cryptocurrencies. Bitcoin, Ripple, Litecoin, and countless other similar currencies now provide wholly anonymous payment methods that are in no way connected to any centralized bank or government. While there is of course even more that can be written on the history and current state of RaaS, ransomware families, and cryptocurrencies, let's dive into some scenarios of ransomware attacks, as well as what can be done to prevent future attacks or mitigate their impact on your business.

Case Study One: Ransomware at a Restaurant

If you're reading this report, you're likely already aware that ransomware is a major business challenge that will not diminish in the near future. If anything, the sophistication and prevalence of ransomware is swiftly increasing. But what does it look like when an organization falls victim?

On the evening of March 19th, 2016, the owner of Hard Times Café in Bethesda, MD, began having problems with their point of sale (POS) system. The following morning, they discovered that their POS system had been compromised by ransomware. They were being asked to pay $10,000 in bitcoin for the release of their encrypted files. When the team contacted the FBI, they were told to pay or rebuild their system since the agency was overwhelmed with ransomware cases. The restaurant was closed for seven days before being able to reopen. Was Hard Times Café specifically targeted? Probably not...and that is where things get truly scary. No matter who you are and what business you run, such indiscriminate targeting means you could be next.

YOUR DATA IS YOUR BUSINESS

Underestimating the necessity of a reliable backup solution can be a financial disaster for large companies, but it can be fatal for smaller ones. During the seven days that Hard Times Café was closed, its three dozen employees went without pay, and the business generated no revenue. In addition, they had to replace the software and hardware that was compromised and file an insurance claim. A company's data protection solution is only as good as its ability to return to business as usual, and the only way to know that you have this ability is to test for it.

TESTING YOUR RECOVERY PLAN

As mentioned above, a good recovery plan is one that you've successfully tested. Large enterprises are often required to test their disaster recovery to maintain compliance with requirements such as HIPAA. But with fewer resources to absorb the impact of a data disaster, it's equally important for smaller companies to follow this practice.

So, what goes into a strong test? Every company has unique needs for disaster recovery. But these are some of the key ideas to keep in mind when creating a plan:

- Know your business: a strong DR plan requires understanding which applications are most critical to supporting your business. In some cases, the most prominent applications may not have the most financial impact when offline. A successful test doesn't just show that data is recoverable, but confirms that a company can quickly operate after a disaster.
- Calculate the cost of disaster: compare the cost of investing in strong protection to earnings lost if your business is offline. One approach is to tier your recovery plan and organize your applications by investment priority. This can help you strategize the roadmap of your DR plan and testing procedures.
- Test, test, and test again: your business changes every single day, and your test plan needs to change with it. Investing in strategies that let you test without interrupting production will allow you to increase the frequency of your testing, ensuring that your documentation can be continuously updated as your business evolves.

There are backup solutions out there that require large amounts of time, manpower, resources, and budget to do reliable testing. When you're seeking out a backup and recovery solution, its testing capabilities are crucial. How long does it take to do a test? How many people on staff are needed to get this done? How much is it going to cost the company? These are all important questions to be able to answer when you are in the market for a backup and recovery solution.

Case Study Two: Not Just Hospitals Hacked

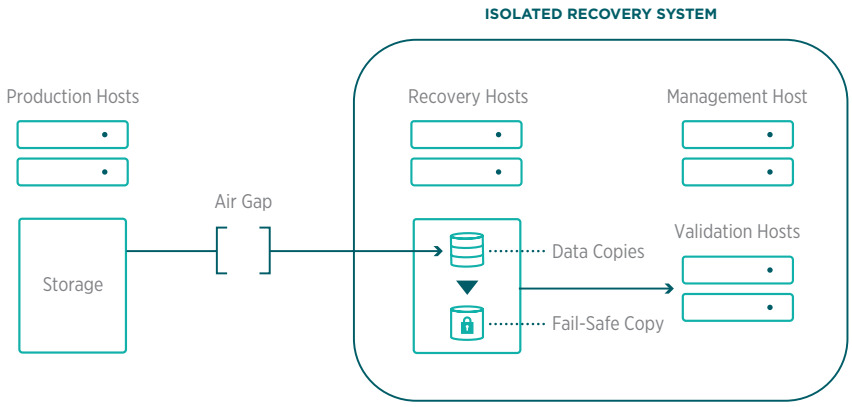
The above exemplifies some of the repercussions of a small-scale ransomware attack. But what happens when the breadth of an attack is much larger and far reaching? In May of 2017, Barts Health Trust, which runs hospitals across the UK, was hit with a massive ransomware attack. The attack began in the middle of the night, and rendered systems completely frozen while files were encrypted. When employees at various hospitals discovered what was going on, they were met with messages that demanded a large amount of bitcoin in order to have files, including sensitive patient data, returned to them. In a hospital setting, the attack's repercussions were extremely severe, as people's medical well-being was at risk. According to The Guardian, "Patient records, appointment schedules, internal phone lines and emails were rendered inaccessible and connections between computers and medical equipment were brought down. Staff were forced to turn to pen and paper and to use their own mobile phones." In addition to the inconvenience, surgeries were postponed, and only patients with urgent issues were able to be treated.

Although they were advised by authorities investigating the crime to avoid paying the ransom which could increase the incentive for future attacks, over £108,000 in bitcoin was paid by victims of this #WannaCry ransomware attack.

The issue here is that most companies are unable to keep every single system up to date at all times. In some cases, when organizations are running old systems, a Windows update that could help protect against ransomware unfortunately causes critical appliances like CT scanners to stop working. This is a frustrating catch-22 for healthcare providers who need to prioritize both patient safety and data security. This dilemma makes the need for fast, reliable recovery all the more business critical.

ISOLATED RECOVERY

Many of the hospitals mentioned were operating on systems that hadn't been updated to prevent against WannaCry, and were lacking completely modernized backup and recovery solutions. To address this, some vendors are pushing the idea of Isolated Recovery. Simply put, there's physical isolation between two networks—most commonly a secured and an unsecured network. Isolated Recovery is built on the concept of having a separate data center infrastructure that is disconnected from the primary infrastructure via an air gap.



In the case of Isolated Recovery, however, the air gap is closed on a regular schedule for replication updates. Think of this as being similar to the operational overhead of a DR infrastructure. In theory, if your files are encrypted by ransomware, there is complete certainty that your air-gapped data isn't affected and is available for restore.

You might already be thinking about update schedules. What if the ransomware isn't detected before the scheduled update occurs? At that point, your separate infrastructure hasn't bought you anything despite its cost and complexity.

Even worse, what if the scheduled update happens after a ransomware infection (or other attack) but before detection? The ransomware may be dormant, specifically to get past regular update windows schedules, and now you have ransomware-encrypted files in both places. In all honesty, we have yet to meet a customer who has experienced real-world benefits with this approach.

What's the real challenge? Based on customer conversations, undetected ransomware file encryption is the main challenge people are trying to protect against when considering Isolated Recovery. So why does immutability matter? Traditional backup systems don't all have the capability to provide snapshots. Alternatively, when using Rubrik, a hybrid cloud application for recovery, search, development, and more, all backups (aka snapshots) are immutable once created. In the words of a security lead at Rubrik, "No amount of compromise to the machines we back up will cause us to do bad things to existing backups." Regardless of subsequent backups, which may include encrypted versions of previously backed-up files, the previous backups are never affected. Additionally, the previous backups are never available in a Read/Write state to the client. Even during a restore of a VM, the underlying backups remain Read Only. This prevents ransomware from being able to access and encrypt backup data.

Immutability is critical—it's what allows Rubrik to meet and exceed the benefits of an air-gapped environment for your backup infrastructure without the operational complexity and higher cost. Even if someone compromises your production infrastructure and deletes items like VMs, file systems, databases, and more, we do not delete the related backups. Instead, they are turned into "relics" inside of Rubrik and aged out over time based on the pre-assigned policy. As you may have realized, the discussion above applies to anyone with a data center today and not just hospitals.

If you'd like to further explore this topic, please refer to our "Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value" paper.

Case Study Three: A Ransomware Attack Prevented

At this point in the report, you may be discouraged by the seemingly ubiquitous nature of ransomware and its frightening ability to target organizations. However, there is hope when it comes to being prepared for and preventing against an attack. Langs Building Supplies, a leading supplier of timber products in South Queensland, Australia, was recently hit by a ransomware attack. Due to its effective backup infrastructure, the company was able to thwart the threat and restore its data without paying a ransom. We sat down with Matthew Day, CIO and Support Manager at Langs Building Supplies, to discuss his experience defending against a ransomware attack.

Q: How were you able to identify that a ransomware attack had occurred?

A: We have monitoring tools in place to send alerts when there are high change rates in the data structure. An alert was triggered, and we were able to shut down the affected VDI desktop within minutes. Because we could stop the attack mid-stream, we were able to prevent the spread of the attack before it got to the rest of the infrastructure.

Q: Can you describe the ransomware attack?

A: This attack entered the system through an email link that was sent to an employee. One of our production file servers had a CryptoLocker placed on it where around 15,000 files were renamed as .encrypted. This meant that these files could not be accessed without a proper passcode.

Q: How were you able to recover your data?

A: Because our data management solution is API-driven, we were able to write a script to restore our files back to the VM from the latest snapshot of the server. This was simple enough. It took under 25 minutes to write, and we had all of our files back to the file server and powered up in approximately one hour. The next day it was as if nothing had ever happened. Having a top-notch data management solution in place means I can go about my day-to-day job without worrying about data loss. I know I have it covered.

Q: What aspects of your current backup solution enabled this recovery to be possible?

A: We've taken steps to ensure our data management solution is top notch precisely to make such occurrences cause less of an interruption. We want to ensure that these types of situations, which you can never prepare enough for, are just minor inconveniences.

1. Modern technology: modern technology does not necessarily mean low-touch but really that it works when you need it, and how you need it to. Our converged backup appliance really helps manage our data. It can easily manage and protect our VMs, set our protection policies as general or as granular as we want, and search across our data protected for specific VMs, objects, or files to restore.
2. Automation via APIs: the typical use case of finding a single file here and there via the UI is simple, but finding thousands of files would have been time consuming. Having a programmatic interface that allows custom workflows for third-party services allows us to automate and orchestrate the management of our environment even further. We were able to write a script to search for and restore our affected files without having to go through a painful dig and recover process manually.
3. Data efficiencies: we can take snapshots more often as less data needs to move to our backup location at any point in time with an incremental-forever approach. This allowed us to discover the exact time when our files were renamed and recover our files from just before the attack occurred.

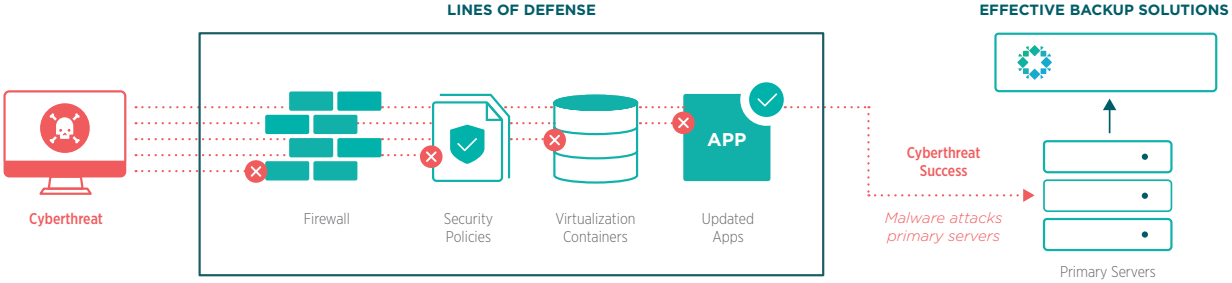
By putting a reliable and effective backup solution in place, cyber threats such as ransomware can be reduced to a mere annoyance rather than a serious business disturbance. As Matt commented, "Having a top-notch data management solution in place means I can go about my day-to-day job without worrying about data loss. I know I have it covered."

WHY ARE ORGANIZATIONS SO VULNERABLE?

The WannaCry case study you just read about exemplifies the many repercussions of a ransomware attack in a hospital environment. To further understand the challenges that organizations face in regards to ransomware we sat down with our internal security team. They explained in detail why data protection and security need to be integrated at the highest standard in a reliable backup solution regardless of your industry sector.

Q: What is the best form of defense for organizations against cyber attacks?

A: As with all information security threats, the best mitigation for ransomware is an in-depth defense. Organizations can reduce the likelihood of infection by maintaining up-to-date software free of known vulnerabilities. By employing technologies such as virtualization or containers, IT organizations may be able to distribute current software without the disruption caused by traditional software updates.



Ideally, systems with access to critical data should be used only for that purpose. Enforcing a security policy to prevent other uses of these systems would dramatically reduce the chance of malware infection via malicious web pages or email attachments. In addition, traditional network defenses such as firewalls should be employed.

Unfortunately, no combination of security measures will completely protect an organization from ransomware or other security breaches. IT organizations need to address this problem with an approach that integrates security and data protection. They should not only make attacks difficult to mount, but also ensure that they have access to their data if an attack is successful. Organizations must maintain reliable and effective backups of their critical data in case of a compromise. With an effective backup solution, ransomware can ideally be reduced to a relatively minor inconvenience with minimal effect on patient care or your business as a whole.

Q: What does a backup solution need to ensure that data is protected?

A: An effective backup solution is reliable, durable, secure, and allows data to be restored near-instantaneously.

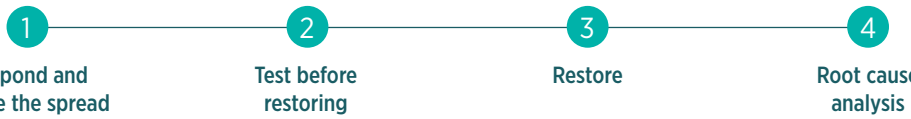
1. A *reliable* solution is one that takes backups at the prescribed interval. Every time. Without exception. In the event of a ransomware infection, this interval represents the maximum length of time over which changes to the data may be lost. For example, a reliable solution configured to take a backup every four hours should always possess a copy of the protected data that is no more than four hours old.
2. A *durable* solution is one that is resilient to low-level failures such as power loss, mechanical hard disk failures, or even critical components such as the CPU or motherboard.
3. A *secure* solution is one that ensures both the privacy and the integrity of the protected data. Only authorized users should be able to restore the contents of a backup, and the solution should prevent a backup from ever being modified. In particular, ransomware running on a system must never be able to delete or encrypt the backups of that system, which would negate the entire purpose of the backup! In an effective backup architecture, a system being backed up should never have the ability to remove its own backups.
4. Finally, an *effective* backup solution must provide near-instantaneous access to the backed up data in order to minimize downtime in the event of an attack or other failure. Any solution that requires the complete contents of a backup to be first restored to a remote system before it can be utilized is, by this definition, ineffective. Particularly when patient data is involved, organizations must be able to live mount and unlock the value of their backups immediately when needed.

Q: How does backup need to evolve so that data protection and security are integrated?

A: The need for significant changes to how backups are managed and protected is imperative. In the last ten years, there has been a lack of innovation while the amount of data growth has been exponential. Legacy architectures are far too complex. Using multiple stacked solutions results in fragmented management and numerous single points of failure that are complicated to address. Additionally, most solutions are not designed for fast data recovery. Often, recovering data can take days or even weeks. A modern backup environment must address these issues as well as ensure data security without reducing the speed and efficiency of its data management.

THE BOTTOM LINE

These are just some practices you can use to help protect your data. The bottom line is that ransomware isn't going away and most customers we speak to, regardless of how many layers of defense are in their environments, admit it's not if but when ransomware will strike and eventually will penetrate the various security layers. Any report you read on ransomware will state that "backups are a must." So, what if you are compromised? Don't panic. Here's what we recommend:



The key here is your response time and getting the affected data back online in the shortest time possible. Rubrik delivers a highly-automated backup with near-instant RTO. But, most importantly, all the backups are immutable, so they can only be read not overwritten. Protecting your valuable data with a highly-automated backup platform is key in having the assurance that, should ransomware infect your environment, you can recover quickly.

WHAT ELSE CAN WE DO?

While there's no fail-safe solution for protecting against ransomware, defense in depth is critical. Below are key steps you can take to prevent ransomware from having detrimental effects on your business:

BEFORE THE ATTACK	
Technology	This could involve next generation firewalls, antivirus, and more.
Education	There are many companies that offer computer security training for employees.
Financial	There are insurance policies available to cover ransomware attacks. Make sure to read the fine print - some require having all patches installed as of the time of the ransomware attack.
AFTER THE ATTACK	
Data Protection	This is where Rubrik can critically help with reliable data protection (enabled by simplicity and immutability) and fast restores (enabled by Live Mount and API capabilities).

Of course, there is far more possible for a defense in depth security strategy.

CONCLUSION

Ransomware is not going away. This makes it imperative for businesses across all industries to adopt a data management strategy of multi-layered security, easy automation, and quick recovery. To learn more about Rubrik and how it can fit into your ransomware protection strategy while simplifying data protection across your entire datacenter, visit www.rubrik.com. As the leading next-generation data protection solution, Rubrik deploys as a plug-and-play appliance in less than an hour and has been adopted across all verticals and organization sizes including Fortune 50 companies.

SOURCES

Gayle, Damien, et al. "NHS Seeks to Recover from Global Cyber-Attack as Security Concerns Resurface." The Guardian, Guardian News and Media, 13 May 2017, www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack.