eBook

05 Lessons Learned

from Ransomware Attacks

Read how five organizations were attacked, how they recovered, and their lessons learned.

COMMVAULT

CONTENTS

Ransomware is headline news. Recent headlines include attacks on an international food processor, a major oil pipeline, a shipping company, hospitals, and municipalities. And maybe you have been personally affected by it. Ransomware strikes all kinds of organizations, from local to global, private to public, and small to large. When it comes right down to it, no enterprise is immune to a ransomware attack.

This eBook examines five ransomware attacks: what happened when they were attacked, how they recovered, and lessons learned. You will gain new insight into securing your enterprise data to avoid becoming headline news.

It’s not if, but when

Are you prepared? Can you successfully recover from ransomware? Consider these facts:

75%	35%	21 Days
of companies infected were running up-to-date endpoint protection[1]	of data remained encrypted after the ransom was paid[2]	Average time firms experienced downtime[3]

[1] PhoenixNAP Global IT Services, 27 Terrifying Ransomware Statistics & Facts You Need to Read, January 31, 2019
[2] Sophos, The State of Ransomware 2021, April 2021
[3] Coveware Quarterly Ransomware Report, February 1, 2021

Data Management Challenges

With inconsistent data security, access, and control across environments, there is an increased risk of data breaches, data leakage, unauthorized access to data, and ransomware. You may be experiencing these challenges:

- **Data fragmentation and lack of visibility**
- **Vulnerable data and data copies**
- **Staff spending too much time chasing issues**
- **Limited or inconsistent recovery options**
- **Multiple tools for management and reporting**

Effective, Multilayered Security Approach

Based on our experience working with thousands of organizations, Commvault believes multilayered security is the best approach to protecting and recovering from ransomware attacks. While the average is 21 days of downtime, we have seen organizations resume operations as quickly as two days when leveraging a multilayered security approach.

One prominent multilayered model is the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which features five layers: Identify, Protect, Monitor, Respond, and Recover. Having multiple layers allows you to tailor the solution to meet your specific IT and business needs. And it provides depth and breadth of coverage against numerous and constantly evolving threat vectors.

01 **Identify**
Create a plan and understand the business impact

02 **Protect**
Design your infrastructure to limit exposure

03 **Monitor**
Single point of view and management

04 **Respond**
Early detection and additional resources

05 **Recover**
Ability to restore anywhere, anytime quickly

COMMVAULT

NIST

National Institute of Standards and
Technology (NIST) Cybersecurity Framework
www.nist.gov

01 Identify

Ransomware Attack: Retail Department Store

CHALLENGE

Ransomware struck an international retail department store, and customers and employees felt its effects.

- 600 stores and an e-commerce site closed
- 130 TB encrypted, impacting 1000+ VMs

SOLUTION

Fortunately, the retailer had a ransomware recovery plan. They immediately contacted Commvault Customer Support, and together they implemented the data-restore operations.

RESULT

Through coordination and teamwork, they achieved:

- A partial recovery in 48 hours, including eCommerce and retail stores
- 100% data restore with zero data loss in 56 hours

> *The ransom is $1 billion.*
> Cybercriminal to a Retail Department Store

Lessons learned

The retailer credits their quick recovery to having a plan and Commvault Complete™ Data Protection. Their post-attack analysis stressed the importance of:

- Test, test, and test again
- Conduct a Business Impact Analysis (BIA)
  - Assess what is the cost of downtime: One minute? One hour? One day?
  - Can we meet our RPO and RTO?

02

Protect

Ransomware Attack: Engineering Consulting Firm

CHALLENGE

An engineering consulting firm was struck by ransomware, which interrupted all customer projects. Worse, they were initially unsure how the virus penetrated their security measures. The attack impacted:

- 500 servers
- All onsite backups

SOLUTION

The firm needed more time to analyze the ransomware attack, identify the vulnerabilities, and close those gaps. They engaged a ransomware negotiator recommended by their cyber insurance company. The negotiator reduced the settlement and, more importantly, bought time to identify and fix the vulnerability.

RESULT

Now they could begin their restore procedures as they had designed offsite air gap copies into their data protection plan. They were able to:

- Restore 498 of 500 servers from the air-gapped backup copies
- Use encryption keys to restore the last two servers in a secure and isolated environment

> “*It’s not personal, it’s just business.*
>
> Cybercriminal to CIO, Engineering Consulting Firm

> “*We paid the ransom as we needed more time.*
>
> CIO, Engineering Consulting Firm

Lessons learned

The firm was protected and successfully restored their data due to:

- A data protection plan that included offsite, air-gapped copies
- Not being dependent on the encryption keys working

03 Monitor

Ransomware Attack: State Government Agency

This story begins three years before the ransomware attack. A state government agency suffered a data loss that prompted reevaluating its data protection and management tools. They consolidated multiple point products to a single solution from Commvault and implemented new tools, resources, policies, and procedures. And they tested to ensure they were ready.

CHALLENGE

The SamSam virus infiltrated the state's Department of Transportation. Its impact was:

- 300 of 3,000 servers were breached, including all databases and applications
- 1,300 workstations were infected

SOLUTION

Commvault software identified the encrypted files first and flagged the activity for an alert. The state's Backup Team immediately notified their Security Team of the suspicious activity, which confirmed a ransomware attack. Next, the state agency:

- Implemented their major incident response plan
- Engaged their IT teams, partners, and Commvault support

RESULT

The agency credited their successful restore to having the right technology partner, right internal team, training, and internal processes in place.

- Network design helped to isolate the virus to one department
- The agency restored 100% of servers with zero data loss

> *"Paying ransom to terrorists is a federal offense. Payment was not an option we were willing to entertain, and we let that be known!*
>
> Sr. Director of Infrastructure Operations, State Government

Lessons learned

- Complete visibility pays off: Commvault monitoring and alerting limited the spread
- Have a comprehensive data protection and recovery plan

04 Respond

Ransomware Attack: National Health Services

CHALLENGE

Ransomware incapacitated a national health services organization. The virus had been lying dormant for two months. Staff overlooked early detection warnings, and then it wreaked havoc:

- Hospitals unable to access their electronic systems, 1,000+ applications
- Radiology and other departments reverted to paper systems
- Patient treatments and services were postponed
- Patient data was published online

> *We were forced to a paper system.*
>
> Sr. Hospital Administrator

> *We will not pay any ransom!*
>
> Head of Government

SOLUTION

The organization was ill-prepared to recover from a cybersecurity attack and lacked a documented response plan. Government and third-party teams were called in to rebuild servers and applications and provide onsite assistance.

RESULT

The organization relied on manual processes and took four months to restore:

- 98.9% applications
- 100% servers

Lessons learned

The Health System performed a complete and public review of the cyberattack. Key findings were:

- Need for executive-level cybersecurity oversight
- Need to establish minimum cybersecurity requirements

Their experience highlights the effect that the lack of planning and inconsistent monitoring can have on an organization's response.

05 Recover

Ransomware Attack: Steel Manufacturing Supplier

CHALLENGE

You could hear the fear in his voice as the IT Manager spoke to his Managed Service Provider (MSP) – not knowing if they could recover from a ransomware attack.

CryptoLocker had hit the organization. A user clicked on an unsuspecting link in an email, and malware quickly spread throughout the organization, infecting files, mail, design, and domain controllers.

SOLUTION

Together, the steel manufacturing supplier and the MSP experts quickly implemented their ransomware recovery plan. They set up a communication center outside of IT to keep all users informed and named the affected user "user 16" to protect their identity.

But there was a problem. They had been in the process of planning a migration from a physical environment, to a virtual environment and plans called for completing the implementation in the next quarter. However, with the impending conversion, OS updates and firmware patches were behind, and in some instances, several versions behind. Jointly, they decided the best option and fastest way to resume business operations was to restore their data to the new virtual environment.

RESULT

By working together and using Commvault data protection and management, they were able to restore their backup copies quickly:

- The majority of services were restored within 72 hours
- Migrated to a fully virtual environment in less than 120 hours

> *We have the data. It'll be alright.*
>
> Manager, Commvault Managed Service Provider

Lessons learned

The lessons may be basic but serve as a great reminder:

- Keep your operating systems and firmware up-to-date
- Maintain redundant systems
- Use your business partners' expertise and additional resources

For this steel manufacturing supplier, what saved the day, was their ability to recover to an entirely new environment. A data protection and management solution that supports flexible recovery options allowed them to recover from a physical to a virtual environment.

How You Can Protect Against and Recover From Ransomware

All five organizations were struck by ransomware, and their results differed. Four organizations were able to recover much more quickly than the 21-day industry average. The National Health Services organization was ill-prepared and took four months to recover. What all five cases highlight is the need for multilayered security:

While you can't control a ransomware attack, you can control how well you protect, detect, and recover from one. Learn how protected you are from a ransomware attack through our risk assessment.

01 **Identify**
Create a plan and understand the business impact

02 **Protect**
Design your infrastructure to limit exposure

03 **Monitor**
Single point of view and management

04 **Respond**
Early detection and additional resources

05 **Recover**
Ability to restore anywhere, anytime quickly

eBook

Let’s protect your business. Visit

COMMVAULT.COM/RANSOMWARE >

commvault.com | 888.746.3849 | get-info@commvault.com

COMMVAULT®