Cove
Data Protection

Ransomware Missteps that Can Cost You

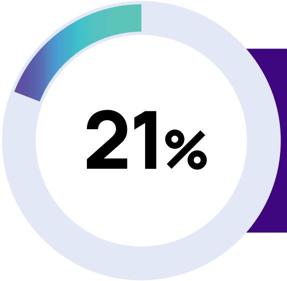
White paper

N-ABLE™

Ransomware Missteps that Can Cost You

Disasters can take many forms, but cyber attacks such as ransomware continue to make headlines, fast becoming the most worrisome type of disaster. IT professionals and managed services providers must be ready to respond in a timely and appropriate manner, and that begins with educating yourself on the major issues and potential missteps that can make a crucial difference.

Cyber security researchers have seen a 21 percent increase in ransomware attacks between Q1 and Q2 of 2022, driven by huge increases in activity from three of the more prolific active operations.[1] The United States was the most targeted region, accounting for almost 40 percent of all incidents. Germany and the UK followed in second and third place.[1]



21%

increase in ransomware attacks between Q1 and Q2 of 2022

Most targeted regions

USA | DE | UK

What kind of disaster is it?

Traditional disasters such as fire, flood, or hardware failure prioritized instant recovery to minimize downtime. While this is still the case in these situations, instant recovery back into the production environment is not the best option in the case of a cyber attack. In this scenario, your network essentially becomes a crime scene, which brings different requirements from traditional disaster recovery.

Consideration	Traditional Disaster	Cyber Attack
Data volume	Comprehensive, all data	Selective, includes foundational services
Recovery	Standard DR/failback	Iterative, selective recovery as part of incident response
Recovery time	Close to instant	Reliable and fast
Recovery point	Ideally continuous	One-day average
Nature of disaster	Flood, power outage, weather	Targeted cyber attack
Impact of disaster	Regional, typically contained	Global, spreads quickly
Topology	Connected, multiple targets	Isolated, in addition to DR

Risk and compliance experts at Arcas Risk Management recommend several key cybersecurity best practices, and in the post-COVID era with increased remote working, the right kind of backup and data protection was added to the critical list alongside tools such as **anti-virus or EDR, firewalls, 24x7 security monitoring, and the use of multi-factor authentication.**

These precautions are especially important considering the degree to which ransomware has been "commercialized," broadening the number of bad actors who can deploy ransomware beyond the highly technical cyber criminals or nation states. It's increasingly clear that this type of crime pays for the perpetrators, and paying the ransom doesn't always guarantee the safe return of data. In fact, demonstrating your willingness to pay can open the door to more attacks, as research shows that 80 percent of organizations that paid a ransom experienced another attack, often at the hands of the same threat actors.[2] Another aspect to consider is that ransomware has evolved to increasingly target backup infrastructure in an attempt to make it difficult for organizations to recover and more likely to pay the ransom.

Recovery as part of incident response

Unlike traditional natural or physical disasters, your recovery plan from a cyber attack should be part of a larger incident response strategy that is much broader than simply recovering from a recent known good backup. Arcas recommends a four-part strategy:

Visibility: If you can't see it, you can't deal with it effectively. The right tools can help you see where the malicious software is lurking in your environment, when it entered, and help you define the path forward. One way to do this is with tools like N-able EDR.

Protection: Even before an attack, it's good practice to review your network segregation, resilient systems and total layered security strategy. This can help protect against future attacks.

Control: Lock down your environment using tools such as multi-factor authentication and ensure you are handling employee de-provisioning, login timeouts, and similar measures to minimize any open doors that attackers can exploit. Also consider applying least privilege by limiting the number of super users, security officers, or admins with API access.

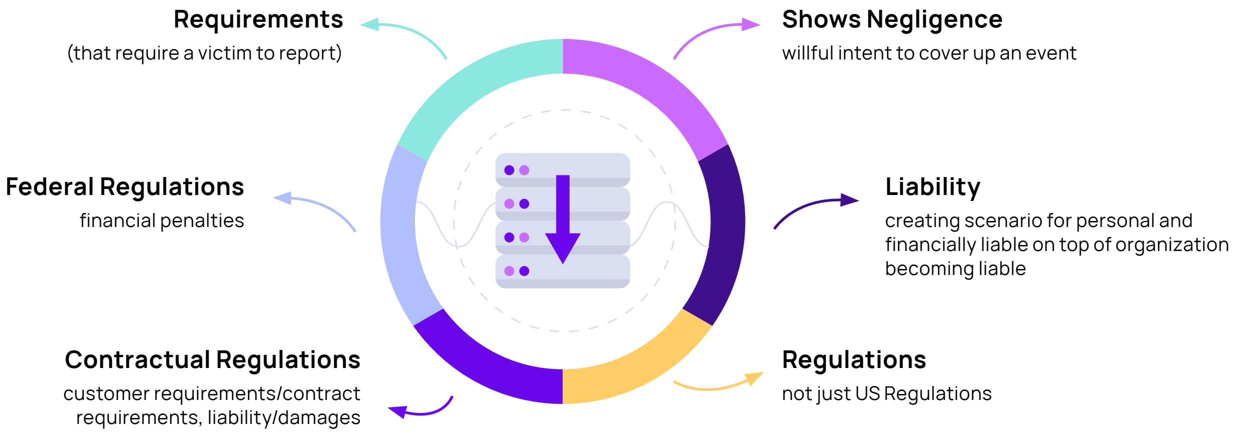
Remediation: Once the immediate threat is handled and neutralized, it's important to assign and clarify remediation responsibilities.

Too often, IT professionals who are focused on traditional disaster recovery may overlook the larger incident response requirements, and fail to coordinate with colleagues on other teams. Tabletop exercises can aid in planning, and better prepare your entire organization for the practically inevitable attacks.

As mentioned previously, a too-hasty “instant restore” back into production can potentially re-introduce malware back into your environment. A better strategy is to recover in a separate, secondary location, so business can resume without impacting forensic investigation by contaminating the ransomware “crime scene.”

Instant Recovery can be costly

(and can cost a company millions)



Requirements
(that require a victim to report)

Shows Negligence
willful intent to cover up an event

Federal Regulations
financial penalties

Liability
creating scenario for personal and financially liable on top of organization becoming liable

Contractual Regulations
customer requirements/contract requirements, liability/damages

Regulations
not just US Regulations

Insurance considerations

Another way to look at ransomware is to realize that at its heart, it is really a risk management problem, not just a technical challenge. This realization has led to an increase in the adoption of cyber insurance, but qualifying for cyber insurance brings additional questions and requirements, as well as benefits.

A cyber insurer is likely to require information about your overall cyber hygiene, including security policies, backups, access control, and event logs. They may also advise investment in crucial management tools, as well as formalization of an incident response team if you do not already have one. They may also provide resources to help educate employees about phishing and other threats.

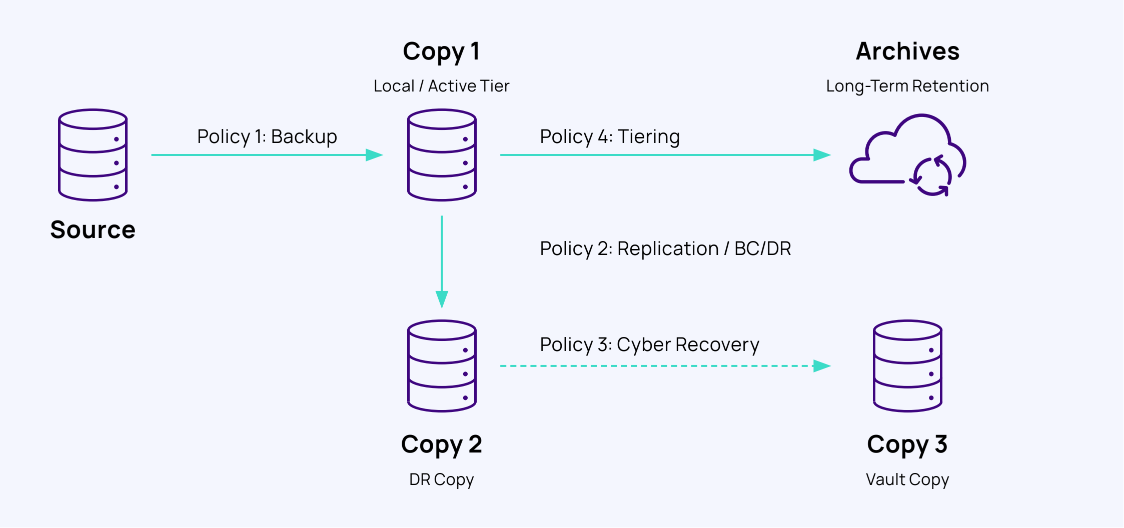
The exercise of qualifying for a cyber insurance policy can, in itself, improve your security posture.

Cyber resilience does not require complexity

Most traditional backup products were designed for physical and natural disasters, and attempts to retrofit them for the modern cyber recovery world have led to more complexity, and more copies of backup data, stored in more places. The reality is that you do not need more copies or more complexity to be ransomware recovery ready. In fact, choosing a cloud-first data protection architecture can reduce your vulnerability by shrinking the network attack surface while simplifying your recovery process.

Legacy backup products were built for local-first backup, storing primary backup copies on the local network. The popular "3-2-1" data protection strategy led to replication or tiering to a second storage location. Next, standby copies were added to a vault in preparation for cyber recovery. Then, when the advantages of cloud storage for resiliency were realized, many backup vendors added the capacity for yet another copy to be tiered to the cloud. This chain of events has led to a complex mix of policies requiring orchestration and significant staff time to maintain all the moving pieces.

Traditional Approach—and What It Means for DR



Protection Stream:

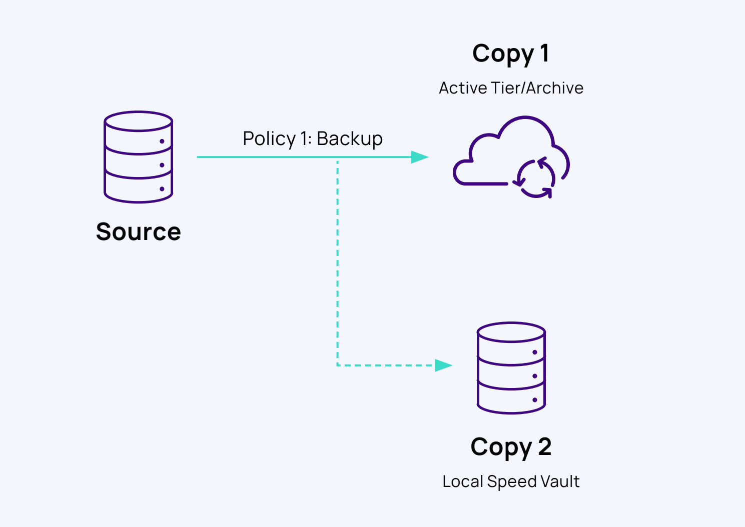
- How do I coordinate four policies?
- Who manages this and how many people do I need?
- Do I need up to four targets?
- Patch orchestration?
- What copies should be immutable?
- How do I protect the backup infrastructure on the primary network?

Recovery Stream:

- How do I create a DR/IR runbook that covers this?
- Consider a table top exercise for this.
- Recovery of the backup catalog if compromised on production?

By contrast, a modern, cloud-first architecture sends each backup directly to the cloud by default, storing primary backup copies off the local network, safely out of the reach of ransomware. You may choose to keep a secondary local copy for faster recovery, but even with this addition, this method dramatically simplifies your policies and reduces operational costs.

Alternate Approach...and what it means for DR



Protection Stream:

- Simplify policies
- Reduce complexity and management overhead
- Shift focus to true DR/IR readiness
- Reduce number of copies >>> Reduce costs
- Benefit from patching as a service
- Offsite copies by default

Recovery Stream:

- Simplify you DR topology and process >>> Simplify your DR/IR runbook
- Flexible restore options for a variety of disasters
- Reduce the attack surface to reduce the likelihood to rebuild your backup catalog

Reducing the size of your attack surface

Cyber criminals will attempt to gain access to your network through a variety of methods. There are several frequently used attack vectors to which traditional on-prem backup applications have proven vulnerable. Some groups and techniques specifically search the local network for backup files from well-known vendors, and delete or encrypt them, thereby cutting off a critical avenue for recovery[3]. They may also delete or disable the backup application server.

By choosing cloud-first data protection as a service, you can reduce your ransomware attack vulnerability in three important ways:

- By storing your primary backup copies in our private cloud, off the local network and far out of the reach of ransomware.
- As a SaaS application, there is no local backup server on the network.
- Mandatory two-factor authentication limits unauthorized access to your backups.

>>> **To learn more about Arcas Risk Management's recommendations** for ransomware readiness, watch this on-demand webinar: https://youtu.be/ON28_27swIo.

>>> **To learn more about how Cove Data Protection's cloud-first data protection** as a service architecture reduces your attack surface, check out this short video: https://youtu.be/c-rHzx-qqTM.

About N-able

N-able fuels IT services providers with powerful software solutions to monitor, manage, and secure their customers' systems, data, and networks. Built on a scalable platform, we offer secure infrastructure and tools to simplify complex ecosystems, as well as resources to navigate evolving IT needs. We help partners excel at every stage of growth, protect their customers, and expand their offerings with an ever-increasing, flexible portfolio of integrations from leading technology providers. n-able.com

[1] https://www.digitalshadows.com/blog-and-research/ransomware-in-q2-2022-ransomware-is-back-in-business

[2] https://www.infosecurity-magazine.com/news/most-ransomware-victims-hit-again/

[3] https://threatpost.com/conti-ransomware-backups/175114/