

THE STATE OF DATA SECURITY

Measuring your
DATA'S RISK



Rubrik Zero Labs



CONTENTS

INTRODUCTION **03**

DATA AND METHODOLOGY **04**

Is Your Data at
RISK FROM ATTACKERS? **14**

Is There
RISK IN YOUR DATA? **19**

How Bad
WILL IT BE? **28**

Recovery
TO RESET **37**

Resetting
DATA RISK **41**

ACKNOWLEDGEMENTS **48**

This is a story about



DATA

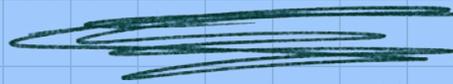
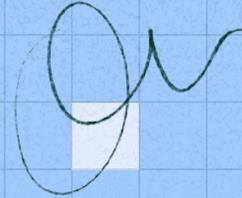
The data types you own, how data changes,
and a pragmatic view of data threats.

It's also a story about risk. How we measure it, our ability
to plan for it, how it changes, and its never-ending presence.

But first, let's explain *how we got here*.



DATA AND METHODOLOGY



Rubrik Zero Labs strives to deliver actionable, vendor-agnostic insights to reduce data security risks. To that end, we incorporated findings from four primary sources.

RUBRIK TELEMETRY = ◆

We utilized Rubrik telemetry in an effort to understand a typical organization's data estate and the risk realities.

WAKEFIELD RESEARCH = ▲

Perspectives from 1,600+ IT and security leaders

RUBRIK PARTNERS = ●

Research and guidance from two Rubrik partner organizations

CONTRIBUTING ORGANIZATIONS = ■

Research from respected cybersecurity organizations and institutions

RUBRIK TELEMETRY ◆

Rubrik Zero Labs believes if organizations trust us with their data, we must be transparent about what their data tells us. Speaking of transparency, here's what makes up our telemetry and how it influences our perspective.

Note: This study contains the first use of Laminar-derived data. Laminar is a leading data security posture management platform acquired by Rubrik in 2023.

RUBRIK TELEMETRY INCLUDES:

6,000+ clients

68 countries

42 EB secured with 38.4+ billion sensitive data records



Total volume of data secured:

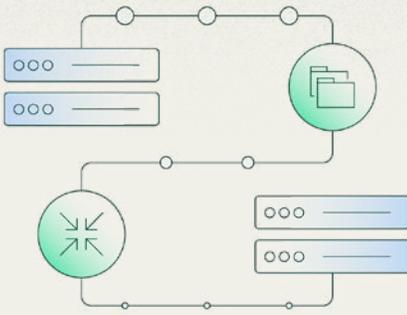
- 42 exabytes of logical storage
- 963 backend petabytes (BEPB) of physical storage



38.4+ billion sensitive data records



Data covers 1 Jan 2023 through 31 Dec 2023



EB vs. BEPB

A reminder from the data nerds: When most of the world hears “data,” they think of logical storage, also known as *frontend* storage. Those of us in the data business focus on *backend* storage. Rubrik takes the entirety of an organization’s data and performs a number of different techniques—including deduplication and compression—to reduce the amount of *frontend* data to *backend* storage. We’ll use backend storage throughout this report.

How much is 42 EB?

Think about your healthcare record with all the forms, images (x-rays, MRIs, etc.), notes, and other data. If you’re like most people, your healthcare record is about 80MB.

If Rubrik’s 42 EB of protected data consisted of nothing but healthcare records, it would be the equivalent of five healthcare records for every one of the 117 billion people who lived on earth for all of humanity’s history. It’s like... a lot.

WAKEFIELD RESEARCH [▲]

We partnered with Wakefield Research to conduct a study that gathered additional insights from both IT and security leaders. This data supplements our Rubrik telemetry to give us insight into both the leaders’ point of view and what they see on the ground. No Rubrik clients are included in this dataset to be as objective as possible.

1,600+ IT and security leaders

10 countries

50%+ CIO or CISOs

1,625

decision-makers at companies with at least 500 employees across 10 countries (United States, UK, France, Germany, Italy, Netherlands, Japan, Australia, Singapore, India) in three regions (Americas, EMEA, and APAC)

50%

CIOs or CISOs

50%

IT decision-makers

50%

Directors or VPs

50%

Security decision-makers

RUBRIK PARTNERS

We leveraged datasets and received guidance from two Rubrik partners in ongoing efforts to improve data resiliency.



Microsoft provided data from the 2023 [Microsoft Digital Defense Report](#)¹, specifically data exfiltration rates and resiliency recommendations.



Aon provided data from the [2023 Aon Cyber Resilience Report](#)², specifically data backup realities and post-intrusion outcomes.

CONTRIBUTING ORGANIZATIONS

Rubrik included key data from various organizations with unique visibility compared to Rubrik telemetry in an effort to provide as objective a view as possible.



Mandiant provided dwell times observed in its incident response/MDR events [across 2023](#)³.



Palo Alto Networks Unit 42 provided findings on ransomware demands and payments from their incident response/MDR events across 2023.



Proofpoint provided information on cloud targeting based on their [2023 Human Factors Threat Report](#)⁴.



Recorded Future provided publicly reported [ransomware trends across 2023](#)⁵.



The University of Minnesota Twin Cities - School of Public Health provided ransomware impacts on public health institutions based on their research "[Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients](#)⁶," which is published and currently undergoing final peer review.

1 <https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023>

2 <https://www.aon.com/2023-cyber-resilience-report/>

3 <https://www.mandiant.com/m-trends>

4 <https://www.proofpoint.com/us/resources/threat-reports/human-factor>

5 <https://therecord.media/ransomware-tracker-the-latest-figures>

6 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292



LET'S TALK ABOUT RISK



Let's set the ground rules for how this study approached risk.

FIRST

We're going to make the "risk math" easy:

What is the likelihood your data will be affected by an external entity



What is the risk resident in your data today



The impact that's likely to produce



Your decisions in response to the impacts



Risk Math

IN YOUR FACE BIG MATH!



SECOND

We're going to focus on data.

As a data security company, our strongest insights involve an organization's data—as opposed to its infrastructure or architecture—so we focus on risks in and to your data.

Specific Focus Areas

Let's be honest. You're busy. None of us have time for a full deep-dive on every aspect of data security. We intentionally narrowed this study to a few key topics:



Cloud

The existence of commercially available clouds can now be measured in decades. Yet, confusion about cloud data security remains. The cloud is targeted with more frequency—and more success—than its on-premises counterparts. It also contains blind spots making it difficult to defend.



Ransomware

Not too long ago, experts predicted ransomware's decline. It didn't really happen, and ransomware continues to wreak havoc on organizations of all kinds.



Healthcare

With few exceptions, healthcare organizations produce and store more sensitive data and are subject to more regulatory scrutiny than other industries. A fringe benefit of the regulatory pressures on healthcare is more publicly available data to study.

THIRD

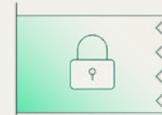
Who is this study for?



Intelligence should inform the right decision-maker, and risk decisions typically happen at the senior-leader level.



Our goal is to inform and aid these senior-leader discussions across business, cybersecurity, and IT functions.



By giving these decision-makers a common place to start from, they'll be better prepared to tackle risk together.

NOW LET'S TALK A LITTLE BIT ABOUT HOW PEOPLE PERCEIVE RISK.



Humans don't deal with uncertainty well. When faced with the possibility of something happening, we like to think either:

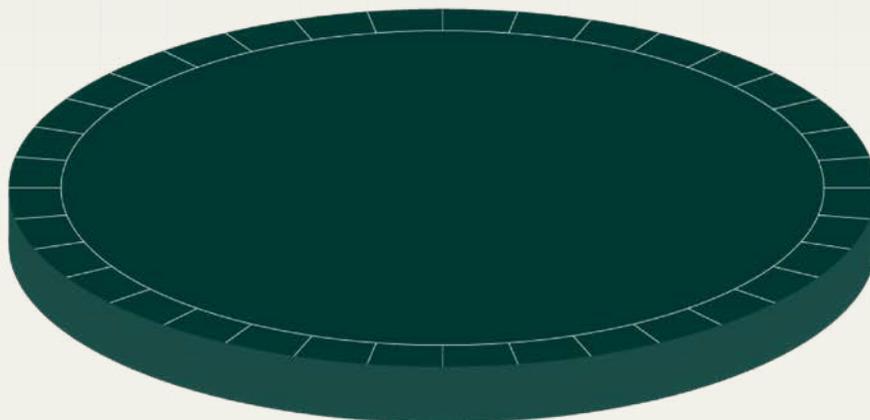
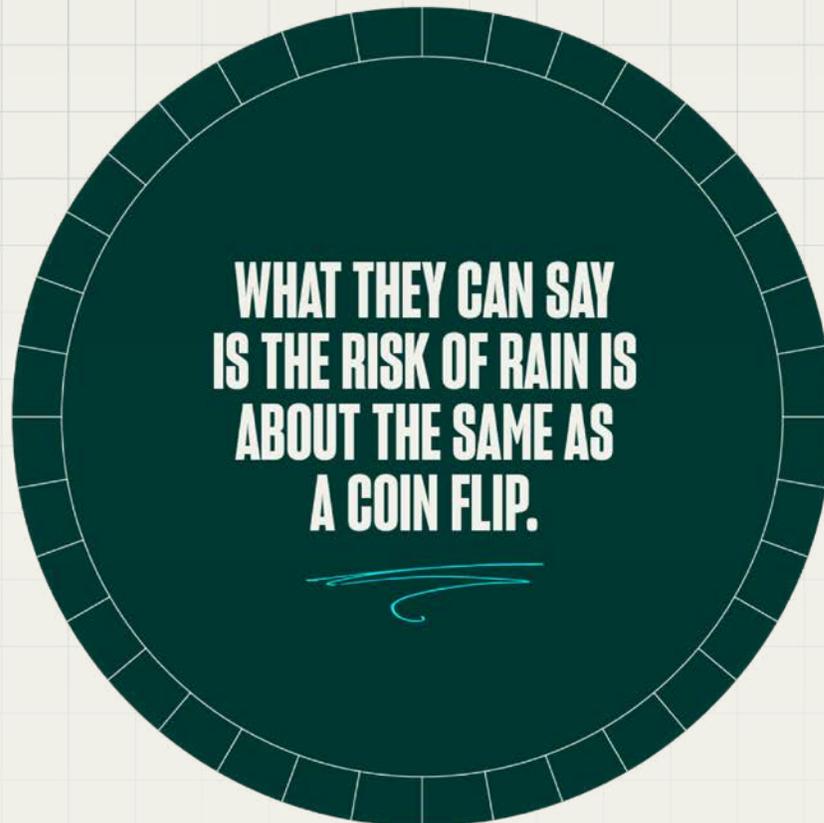
“YES, THIS MOST DEFINITELY WILL HAPPEN.”

IN REALITY, THINGS ARE A BIT MORE SQUISHY

“NO, THIS DEFINITELY WON'T HAPPEN.”



If a meteorologist tells you there's a 52% chance of rain in your area, they're not telling you definitively, "Yes, it will rain," or "No, it won't."





Then there's the details we really want:
How much rain? Is it a sprinkling or a
deluge? Do I just stay home? Because I
didn't want to go to the office anyway.

*These decisions are yours and
yours alone.*

It would be nice if you only had to make
these decisions once.

But ... it just doesn't work that way.

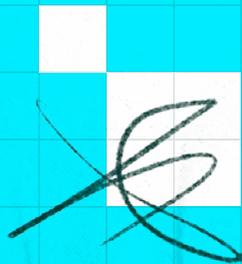
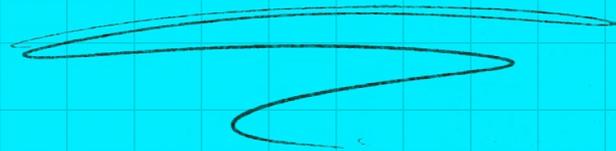
Today's reaction to rain impacts how we think about tomorrow's weather report and also provides lessons learned in dealing with the rain.

These factors combine to set new conditions the next time we have to tackle the storm. That's true of the rain, and it's true of cyber risk.

Let's start with the external threats you should consider.



Is Your Data at
RISK FROM ATTACKERS?



Let's start with a basic question:

Are attackers likely to target *my data*?

Is Your Internet-Connected Fridge Trying to Kill You?

Ransomware Shifting to ESXi is a Massive Evolution

How Attackers are Really Using AI

HOW MUCH OF YOUR NEWSFEED IS REAL VERSUS FUD?

Is This the Next Solarwinds?

The Mother of All Data Breaches: Biggest Data Loss Ever

(Fear, Uncertainty, Doubt)

Why Strawberry Tempest is Worse than Lapsus\$

Nobody can tell you with 100% certainty if you'll be hit with a cyberattack, but we can tell you what happened to your peers last year.

Almost all your peers dealt with cyberattacks about every other week.

Here's what last year looked like across IT and security leaders: ▲

94% of IT and security leaders reported their organization experienced a significant cyberattack last year.

30 The average frequency was 30 malicious events brought to senior leaders' attention across 2023.

93% of external organizations conducted a formal data loss notification to a governing organization.



Cyberattacks are far more likely than *physical theft or fire*.



To put the likelihood of cyberattacks into perspective, a European insurance company¹ compared cyberattacks to traditional threats in the same timeframe and found:

67% Organizations are 67% more likely to experience a cyberattack than physical theft.

5x Organizations are five times more likely to experience a cyberattack than a fire.

20% of organizations do not know what actions to take in the event of a cyberattack.

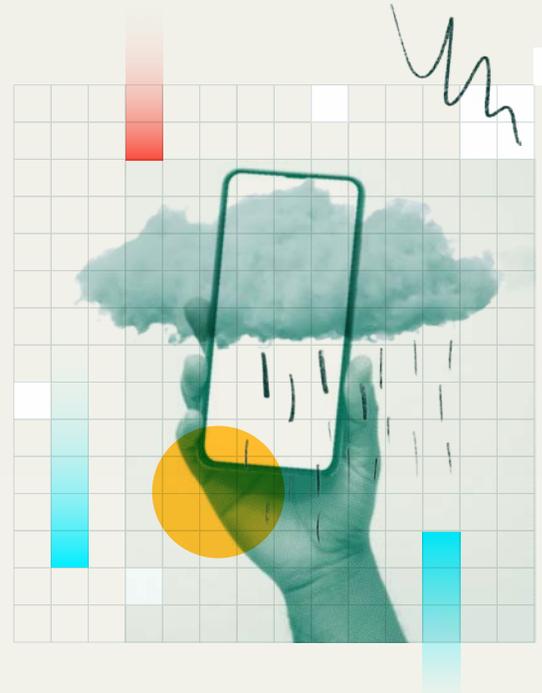
¹ <https://www.aviva.com/newsroom/news-releases/2023/12/One-in-five-businesses-have-been-victims-of-cyber-attack-in-the-last-year/>

Attackers are comfortable targeting *hybrid environments*.

So if you're likely to be targeted, it's useful to understand where and what is likely to happen. Of the 94% of external organizations victimized in a cyberattack, many were attacked across multiple environment types: ▲



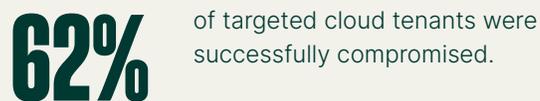
And here's some perspective on the two most common types of attacks in these environments: ▲



Almost all cloud tenants were targeted, and 2 out of 3 were compromised in 2023.



We didn't just find this in our own research. Proofpoint reported¹: ■



1 <https://www.proofpoint.com/us/resources/threat-reports/human-factor>

Attackers have *access to your data* for days before being found

Mandiant measures dwell time¹ as the number of days an attacker is present in a victim's environment before detection.

10 DAYS

The global median dwell time across all events was 10 days last year.

5 DAYS

The global median dwell time for a ransomware event is 5 days.



THE GOOD NEWS:

These are the shortest dwell times ever observed by Mandiant.

THE BAD NEWS:

This still represents a significant length of time for malicious actors to accomplish their goals.

YOU'RE NOT IMAGINING IT. THERE'S MORE RANSOMWARE (70% MORE).¹

Recorded Future tracked a significant increase in publicly reported ransomware attacks last year:

46%



358 reported ransomware attacks against healthcare (46% increase YoY).

70%



4,399 reported attacks across all industries (70% increase YoY).

Now let's shift our focus and look at your data.

¹ <https://www.mandiant.com/m-trends>



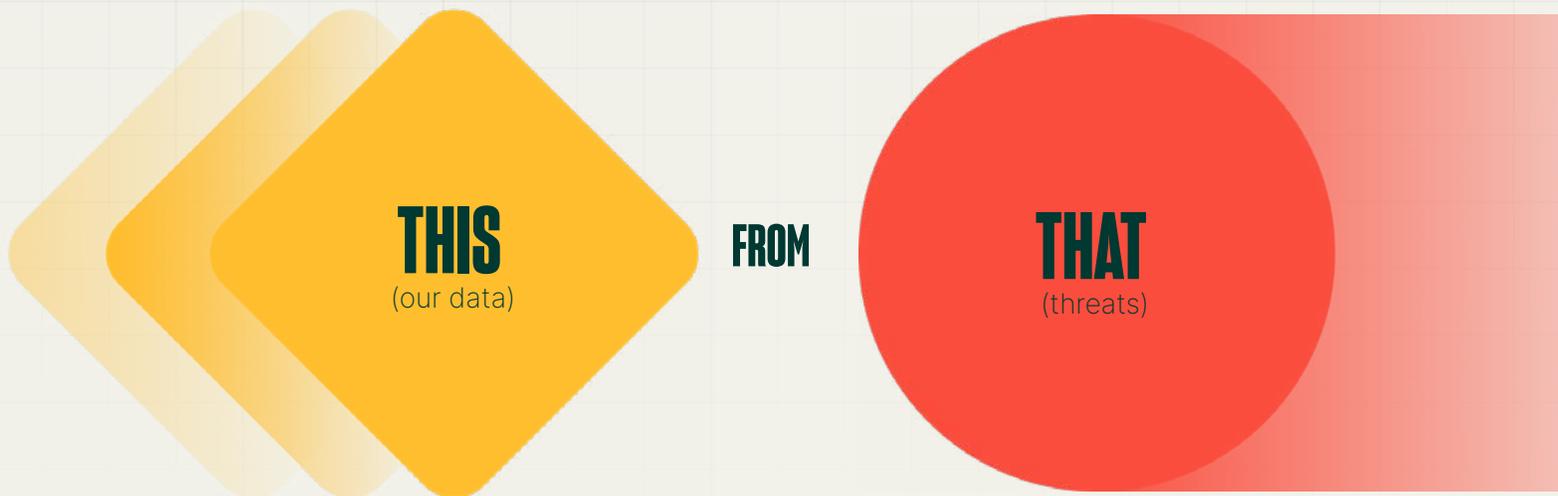
Is There
RISK IN YOUR DATA?

If you know the odds of an attack (and let's face it, they aren't great), it makes sense to do everything you can to minimize your risk by reducing:

THE LIKELIHOOD OF AN ATTACK SUCCEEDING

THE **FALLOUT** FROM AN ATTACK

At the end of the day, what we're trying to do is deceptively simple (on paper). We're trying to protect:



We must examine both sides of that equation. Let's take a look at what our operations expect our defenders to secure.

DATA

is growing rapidly and expanding the defensive boundaries.

Healthcare defenders are responsible for securing a larger data surface area, with more sensitive data, and that is growing faster than the global average. ♦

Healthcare organizations secure 22% more data than the global average.



WHAT'S A BETB AGAIN?

EB vs BEBP

A reminder from the data nerds: When most of the world hears “data,” they think of logical storage, also known as *frontend* storage. Those of us in the data business focus on *backend* storage. Rubrik takes the entirety of an organization’s data and performs a number of different techniques—including deduplication and compression—to reduce the amount of *frontend* data to *backend* storage. We’ll use backend storage throughout this report.

The typical healthcare organization saw their data estate grow by 27% last year (23% for a global organization).



A typical healthcare organization has 50% more sensitive data than the global average.



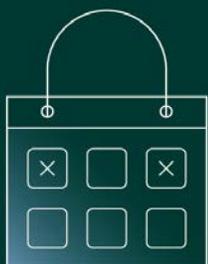
Sensitive data records in healthcare grew by more than 63% in 2023—far surpassing any other industry and more than five times the global average (13%).



ORGANIZATIONS HAD A RECORD-SETTING NUMBER OF ISSUES TO TACKLE LAST YEAR.

Vulnerabilities are not a perfect exposure measure, but they do provide a solid view on the scope and scale of inherited risk from vendors.

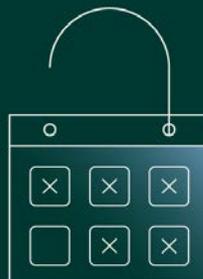
2022 was a record-setting vulnerability year with the highest reported amount ever:



25,083

vulnerabilities discovered

2023 set a new record, a 16% increase over the previous record.



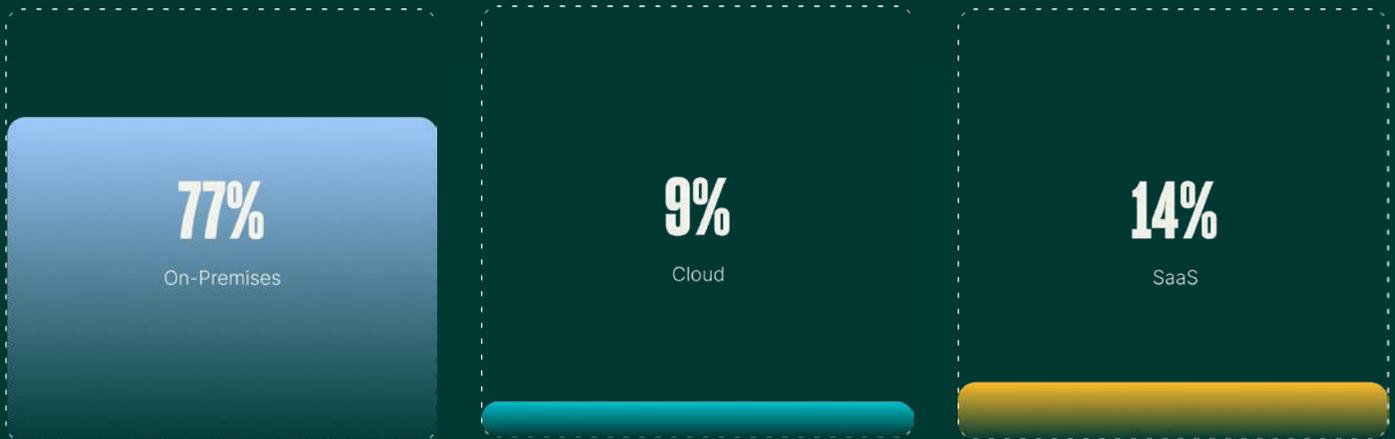
29,065

vulnerabilities discovered

ORGANIZATIONS ARE BECOMING MORE DEPENDENT ON CLOUD AND SAAS [◆]

Demands on a modern business necessitate an increased focus on the cloud. We see the nature of hybrid environments consistently moving towards cloud and SaaS while deprioritizing on-premises architecture growth.

2022:



2023:



THE CLOUD CONTAINS SECURITY BLIND SPOTS

Cloud Data Security

BLIND SPOT #1:

70% of all data in a typical cloud instance is object storage. ♦

Object storage represents a common blind spot for most security appliances because it's typically not machine readable by these same technologies.

Cloud Data Security

BLIND SPOT #2:

88% of all data in object storage is either text files or semi-structured files, such as CSV, JSON, and XML. ♦

So let's assume your tooling and processes can see inside object storage. Here's another issue: Unstructured data (such as text files) and semi-structured data represent another blind spot for security because these data types vary wildly in being machine readable and/or covered by prominent security technologies and services.

Cloud Data Security

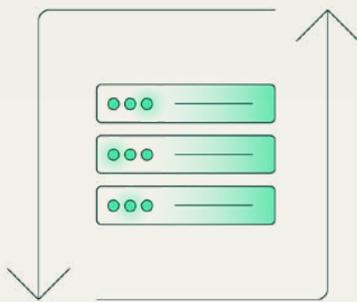
BLIND SPOT #3:

More than 25% of all object stores contain data covered by regulatory or legal requirements, such as protected health information (PHI) and personally identifiable information (PII). ♦

Put simply, the cloud comes with inherent risk because organizations need it to function, but it also stores regulated data with fewer security capabilities and less visibility than on-premises assets.

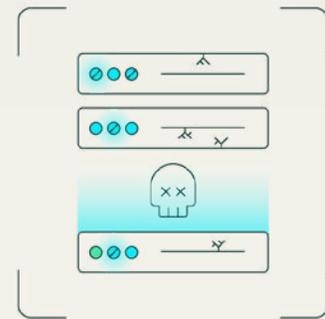
MOST BACKUP SOLUTIONS ARE NOT UP TO THE TASK.

Backup and recovery technologies are critical components for virtually all organizations. They've been used for disaster recovery and business compliance for decades. However, most organizations struggle getting these solutions to actually work.



99%

Rubrik Zero Labs previously stated¹ more than 99% of external organizations reported having an existing backup solution. ♦



93%+

However more than 93% of these organizations encountered significant issues with their existing solution. ♦



70%

Aon reported² 70% of organizations do not store backups offsite or their backups are not immutable. •



40%

Almost 40% of Rubrik-observed organizations have not set compliance policies for their data backups. ♦

1 <https://www.rubrik.com/zero-labs/2023-spring>

2 <https://www.aon.com/2023-cyber-resilience-report/>

BAD NEWS:

Cybercriminals are hip to the backup game and routinely target backups.

Attackers almost universally attempted to remove backup and recovery options from defenders.

External organizations that reported a successful attack observed: ^

96%

Attackers tried to affect the backups in 96% of these attacks.

74%

And were at least partially successful in 74% of those attempts.

Cybercriminals are taking out insurance policies against effective restores

Attackers are evolving their approach to ransomware based on defender actions. Instead of simply encrypting data, cybercriminals also steal data and threaten to publish it. If their target can thwart the encryption event with a swift recovery, ransomware actors have another way to drive a payout.

2x

Microsoft determined the number of times threat actors potentially exfiltrated data after an initial compromise has doubled since November 2022. •

12%

Aon assessed data breaches have a 12% higher overall impact on organizations than ransomware alone. •

93%

93% of external organizations that endured a successful ransomware attack reported paying a ransom demand with 58% of these payments motivated by threats to leak stolen data. ▲

Now that we know the likelihood, let's take a look at the impact.



How Bad
WILL IT BE?





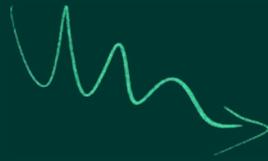
Folks often think
the cyberattack is
the end of the story.

But it's really
the middle.



Going back to our weather forecast example, the story of your day *doesn't end when it rains*.

You still have to live your life. But now you need to adjust to the conditions. How are you going to stay dry? Does the dog get walked in the rain? What happens when you inevitably get rained on?



Likewise, a cyberattack sets off a whole slew of remediation, recovery, and reporting efforts.

How painful these efforts are depends on how well you prepared for these outcomes in the first place.

Let's look at the fallout from cyberattacks, specifically ransomware, against healthcare organizations last year.

THIS IS WHAT HAPPENS AFTER THE CYBERATTACK.

Approximately 1 in 3 Americans had their personal records compromised during healthcare intrusions last year¹.



people (on average) were affected during a single cyberattack against healthcare last year.

186%
increase from 2022

133M+

people had their records compromised from cyberattacks against U.S. healthcare organizations last year.

¹ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Ransomware attacks on healthcare organizations impact almost five times more sensitive data than the global average. ♦

Rubrik measures both the ransomware encryption blast radius and the sensitive data impacted by this blast radius. Impacted files include encrypted files, deleted files, and exfiltrated files.

Here's the impacted data for a typical healthcare ransomware encryption event in a production environment:

Healthcare organizations:

16.8M

total impacted files per encryption event.

8.4M

sensitive data records within these impacted files.

20%

of a typical healthcare organization's total sensitive data holdings impacted every time there is a successful ransomware encryption event.

The average global organization at large typically experiences a much smaller impact to its sensitive data.

13.7M

total impacted files per event

1.7M

million sensitive data records affected per encryption event

6%

of an organization's total sensitive data

Virtualization really matters for healthcare and ransomware. ♦

Now let's examine where ransomware encryption happens.

97%

of healthcare encrypted data is within virtualized architecture.

83%

of all industries' encrypted data is within virtualized architecture.

This is likely driven by two factors.

- 1:** Virtualized architectures typically have less security coverage compared to traditional endpoints. This creates security dead spots and simultaneously allows attackers unfettered access.
- 2:** Once attackers gain access to virtualization control panels, they can often move at speed and scale using only compromised credentials.



RANSOM PAYMENTS VARY WILDLY.

Initial ransom demands are often higher than the actual payouts. Palo Alto Networks Unit 42 noted the following trends in ransom payments across last year: ■

	ALL INDUSTRIES:	HEALTHCARE:
Median demand	\$800,000	\$200,000
Median payment	\$275,000	\$100,000
Median of Top Five Largest Payments	\$25,000,000	\$297,000

Backups and data theft greatly affect a victim's likelihood to pay a ransom.

The University of Twente¹ studied factors that caused victims to pay a ransom and separately what impacted the size of an actual ransom payment. Their findings indicated:

Organizations with recoverable backups were



¹ <https://databreaches.net/university-of-twente-maps-decision-making-process-for-ransomware-victims/#:~:text=for%20the%20best-,article,->

Data exfiltration led to a higher likelihood of paying a ransom and higher ransom payment amounts.

40%

Paid the ransom with data exfiltration.

25%

Paid the ransom without data exfiltration.

5.5x

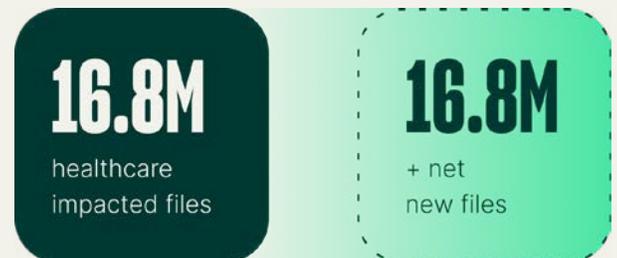
larger ransom payments were made when data exfiltration was involved, compared to encryption-only events.

Storage overload: The recovery blindside nobody sees coming

When it rains, it pours. Few organizations are prepared for the data deluge caused by ransomware.

If a single healthcare ransomware event encrypts or modifies 16.8 million files, it essentially means the encryption event created 16.8 million “new” files for the victim (compared to 13.7 million new files for a typical global organization). ♦

These files are backed up as new files, which consumes vast amounts of storage capacity at the moment of the encryption event.



If a victim's pre-ransomware storage is over 70% capacity, this "new" data could max out an organization's recovery capacity within one to two weeks. ♦



To make this problem more profound, ransomware victims often need to create more "new data," such as: forensic images for analysis and immutable copies for legal purposes. In many cases, response/recovery workflows also require duplicate data. Put simply, a victim must create even more new data as part of the response process immediately after the attacker created a large amount of new data.

In the 200+ recovery operations in the Rubrik Ransomware Response Team's history, this issue typically leads to one of two outcomes. The organization either needs to:

1: Rapidly increase data capacity, which requires financial investments and workforce pressures.

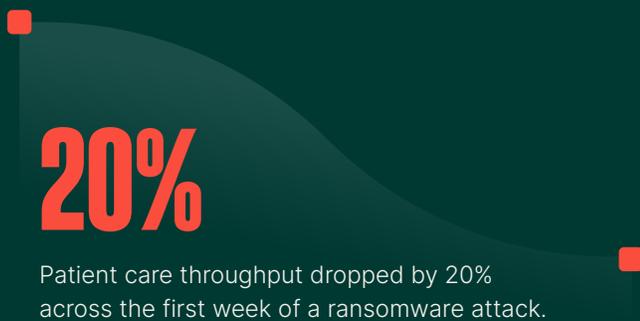
2: Degrade recovery capabilities to slow data growth, which in turn limits recovery options in critical timeframes.



RANSOMWARE FALLOUT DIRECTLY CONTRIBUTED TO AT LEAST 42 US DEATHS.

In any ransomware event, there's the data impact. The real risks—particularly for healthcare—are also measured in operational impacts and lives. ■

The University of Minnesota Twin Cities - School of Public Health studied real-world impacts to hospitals and patient care caused by ransomware events between 2016 and 2021¹. They found:



These attacks aren't just affecting data, businesses, or individual privacy anymore. There's direct evidence cyberattacks are a life and death issue.

1 in 4

While only 5% of US hospitals were directly affected by ransomware during the study's timeframe, an additional 20% of hospitals suffered ripple effects when patients were transferred or diverted from the victim hospitals to surrounding hospitals.

0.5-1%

A typical hospital lost between 0.5 and 1% of their total annual revenue as a direct result of a single ransomware attack.

2-3 wks

Hospitals averaged two to three weeks for a return to typical patient care levels following a ransomware attack.

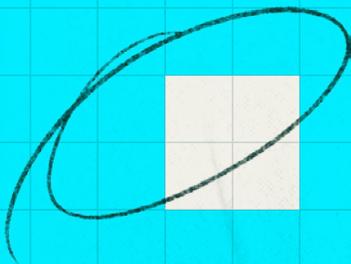
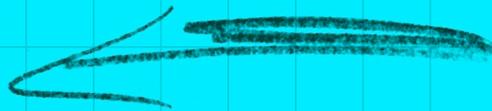
42-67 deaths

The fallout from ransomware attacks directly contributed to the deaths of between 42 and 67 patients².

¹ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292
² <https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/>



Recovery **TO RESET**



After the initial response is done and organizations return to relatively normal operations, the fallout from a ransomware attack continues producing risk impacts.

THERE'S BAD NEWS AND GOOD NEWS HERE FOR US.



Cyberattacks *impact* our organizations and people.

Aon reported a major cyber incident resulted in a:



decrease in shareholder value per event.

External organizations reported the following direct impacts from cyberattacks: ▲



Leadership forced to change



Negative press and/or reputational damage



Lost revenue



Customer Loss

96% of senior IT and security leaders reported changes to their emotional and/or psychological state as a direct result of a cyberattack: ▲



Increased anxiety pertaining to current role



Loss of trust amongst colleagues and team members



Worry over job security



Loss of sleep or trouble sleeping

Executives will need to be convinced their organizations *can recover from the next* attack.

60%

of IT and security leaders are extremely or very concerned about their organization's ability to maintain business continuity during a cyberattack. ▲

28%

of external organizations believe their Board of Directors or C-suite has little to no confidence in the organization's ability to recover critical data and applications in a cyberattack. ▲

CYBERATTACKS PRODUCE PREDICTABLE PROBLEMS TO SOLVE.

Here are the most frequently identified problems during a cyberattack and the most common changes organizations should prepare to encounter after a cyberattack:

External organizations provided the single biggest limitations they faced during a cyberattack: ▲

19%

Issues working across a hybrid environment

18%

Lack of alignment across teams

18%

Ineffective backup and recovery solutions

17%

Lack of leadership involvement

16%

Visibility challenges

These are the most common changes external organizations encountered because of a cyberattack: ▲

24%

Increased senior leader scrutiny

20%

Changes in cybersecurity technology

19%

Reworking cybersecurity plans and procedures

19%

Increased accountability enforcement

18%

Drop in morale among IT or cybersecurity teams

Cyberattacks can drive positive outcomes.

Organizations prepared to capitalize on these crisis moments can reshape their future.

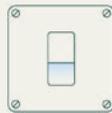
Aon reported companies that successfully navigated a cyberattack saw an **18% shareholder** value increase compared to their peers. •

After a cyberattack, external organizations reported ▲



55%

Increased spending on new technologies or services



42%

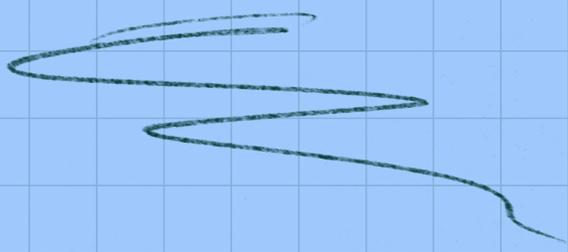
Switched vendors or third party relationships



37%

Hired additional staff

You cannot eliminate risk, but you can influence the risk cycle and affect your new risk baseline.



Resetting
DATA RISK



We'd love to tell
everyone those final
outcomes end the story,



but in truth it's the
beginning of another
chapter.

JUST BECAUSE YOU WEATHERED ONE STORM DOESN'T MEAN IT'LL BE THE LAST ONE YOU FACE.

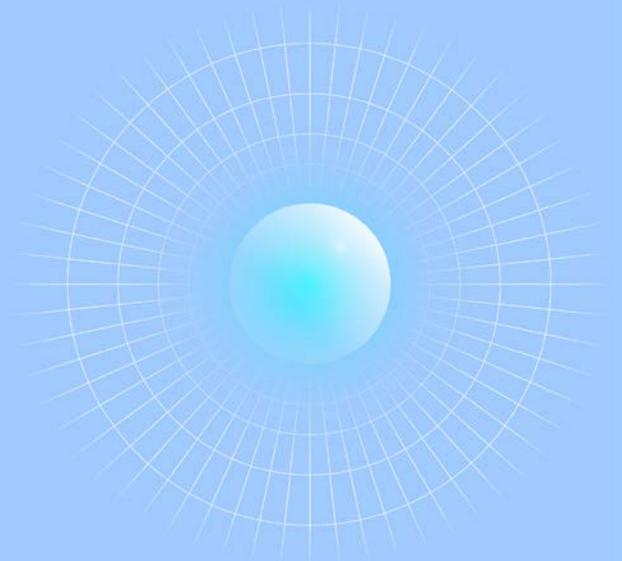
In fact, you'll almost certainly encounter another one and that storm will bring new, perhaps unforeseen risks, with the potential to catch you off-guard.



We'd also love to tell you there are options to change the risk factors controlled by the attackers, but unfortunately our analysis tells us that pursuit is almost as futile as trying to control the weather.

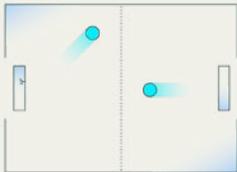
Like most things in life, you cannot control what happens to you, but the good news is you can control the risk reset and subsequent impacts.

Let's dig into the data on how to successfully navigate the risk reset. Each of the risk recommendations is derived from findings about the cyberattacks, the data impacts, or the expected outcomes.

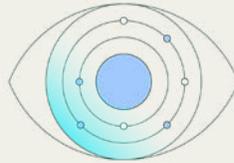


WHAT ACTUALLY IMPACTS YOUR NEW DATA RISK?

Here are the most impactful levers you can pull to significantly improve your data risk:

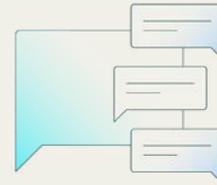


Prepare to challenge attackers across all aspects of a hybrid environment. Attackers are already working successfully in hybrid environments, and our organizations are moving that way.

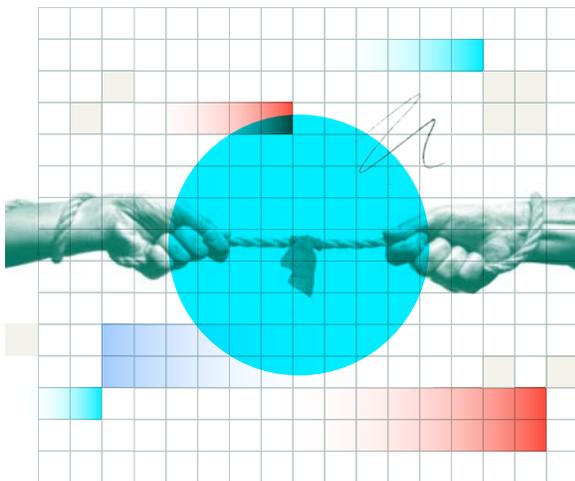


Increase your *data visibility*, specifically:

- Expand your view across all aspects of hybrid environments.
- Know where your sensitive data is located and what type of regulatory aspects apply to specific data elements.
- Prepare to address new leader scrutiny and demonstrate how recent investments will lead to anticipated outcomes.



Anticipate increased leadership scrutiny and proactively communicate your efforts following a cyberattack.



Prepare to recover, and prepare for attackers to *contest your recovery*.

This includes:

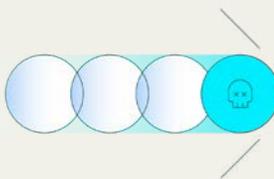
- Ensure backups are fully immutable and available during a cyberattack.
- Automate as much of the recovery process as possible.
- Test recovery outcomes across hybrid environments.
- Leverage existing security services and technologies to test the immutability and integration of backup technologies.



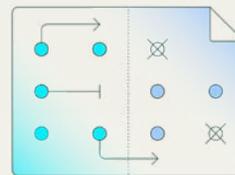
Know your data (especially your sensitive data) is growing. Learn to control that growth and prioritize the defense of critical data.



Prepare to answer regulatory and legal questions in the middle of a ransomware event with an actively encrypted environment and attackers threatening to leak stolen data.



Know that cyberattacks often lead to new technology, increased staff, and switching vendors or partners. Be prepared to capitalize on these change periods to make the most impact.



Communicate plans and outcomes regularly across your entire organization to address dropping morale from cyberattacks and re-install confidence across teams.



Find ways to *unify different teams* before, during, and after a cyberattack.

This includes:

- Create combined playbooks and perform tabletop exercises.
- Determine which team is best suited for specific risk decisions.
- Establish the best way to get the right data to the assigned risk owner.
- Ensure all teams have the same data viewpoint to enable faster decisions and decrease potential resistance from competing viewpoints.

ANOTHER PERSPECTIVE

Admittedly, Rubrik Zero Labs approaches risk from a data-driven perspective. Let's expand our view to include key resiliency recommendations from Microsoft's 2023 Digital Defense Report¹. Microsoft's vantage point is decidedly different from Rubrik's, which in turn, we hope, strengthens risk reduction efforts.

99%

Microsoft assesses basic security hygiene for data will protect against 99% of all attacks.[•]

Specific recommendations are: [•]

- Enable multi-factor authentication
- Apply zero trust principles especially for assets securing critical data and functions
- Use extended detection and antimalware to cover critical parts of hybrid environments
- Keep up to date on patching key systems and applications
- Protect your data by understanding what data is critical, where is it located, and implementing appropriate defensive measures for these enclaves

If we dive one level deeper to Microsoft's view on ransomware, they advocate for "The Foundational Five" as the best path to eliminate ransomware impacts: [•]

1

Modern authentications with phish-resistant credentials

2

Least privileged access applied to the entire technology stack

3

Threat and risk-free environments

4

Posture management for compliance and the health of devices, services, and assets

5

Automatic cloud backup and file-syncing for user and business-critical data

We started this report by simplifying our risk math:
We need to defend THIS from THAT.

In practice, risk is an incredibly complex topic

**WHERE
ONE MASSIVELY
COMPLICATED SURFACE
AREA (YOUR DATA)**

**COLLIDES
WITH**

**ANOTHER
EQUALLY NUANCED AND
CONSTANTLY CHANGING
THREAT SURFACE AREA.**

RISK

Because of the literal millions of variables involved, you'll never be able to fully pin down your risk—or completely eliminate it.

What you can do is get a handle on the most impactful levers, work to address predictable outcomes, and take distinct actions to change the risk calculus in your favor.

We hope this study provided some insight on data risk reduction and prepares you for the evolving risk cycle.

ACKNOWLEDGEMENTS

Rubrik would like to extend our appreciation to the organizations providing their hard-earned data knowledge to this study.

- Our partners at Microsoft and Aon provided both strategic direction and supporting data.
- The following organizations allowed us to use their analysis and provided clarifying material to ensure appropriate categorizations:
 - Proofpoint
 - Recorded Future (Allan “Ransomware Sommelier” Liska)
 - Mandiant (Kirstie “Swiftie” Failey)
 - Palo Alto Networks Unit 42 (Ingrid Parker)
- The University of Minnesota Twin Cities School of Public Health (Hannah Neprash, Claire McGlave, and Sayeh Nikpay) allowed us to leverage their findings, provided a deepdive into their research, and worked with Rubrik Zero Labs to ensure their academic research aligned with Rubrik Zero Labs industry research.

As with all things Rubrik Zero Labs, it takes a village to pull off these studies. Wakefield Research provided external data to make this research as objective as possible. Shaped By found a way to take the data and bring it to life. Finally, many Rubrikans worked hard to provide capability, context, and guidance. We’d like to extend a specific appreciation to Amanda “Danger” O’Callaghan, Linda “Taskmaster” Nguyen, Lynda “Go Niners” Hall, Ben Long, Peter “I’m the Law” Chang, Ajay Kumar Gaddam, Ryan Goss, Derek Morefield, Josh Burns, Gunakar Goswami, Prasath Mani, Ethan Hagan, Kevin Nguyen, Caleb “Social King” Tolin, Kelly Cooper, Hannah Battillo, Sindhu Nagendra, Caitlin “Plz stop letting Steve talk to reporters” O’Malley, and Fareed Fityan.

