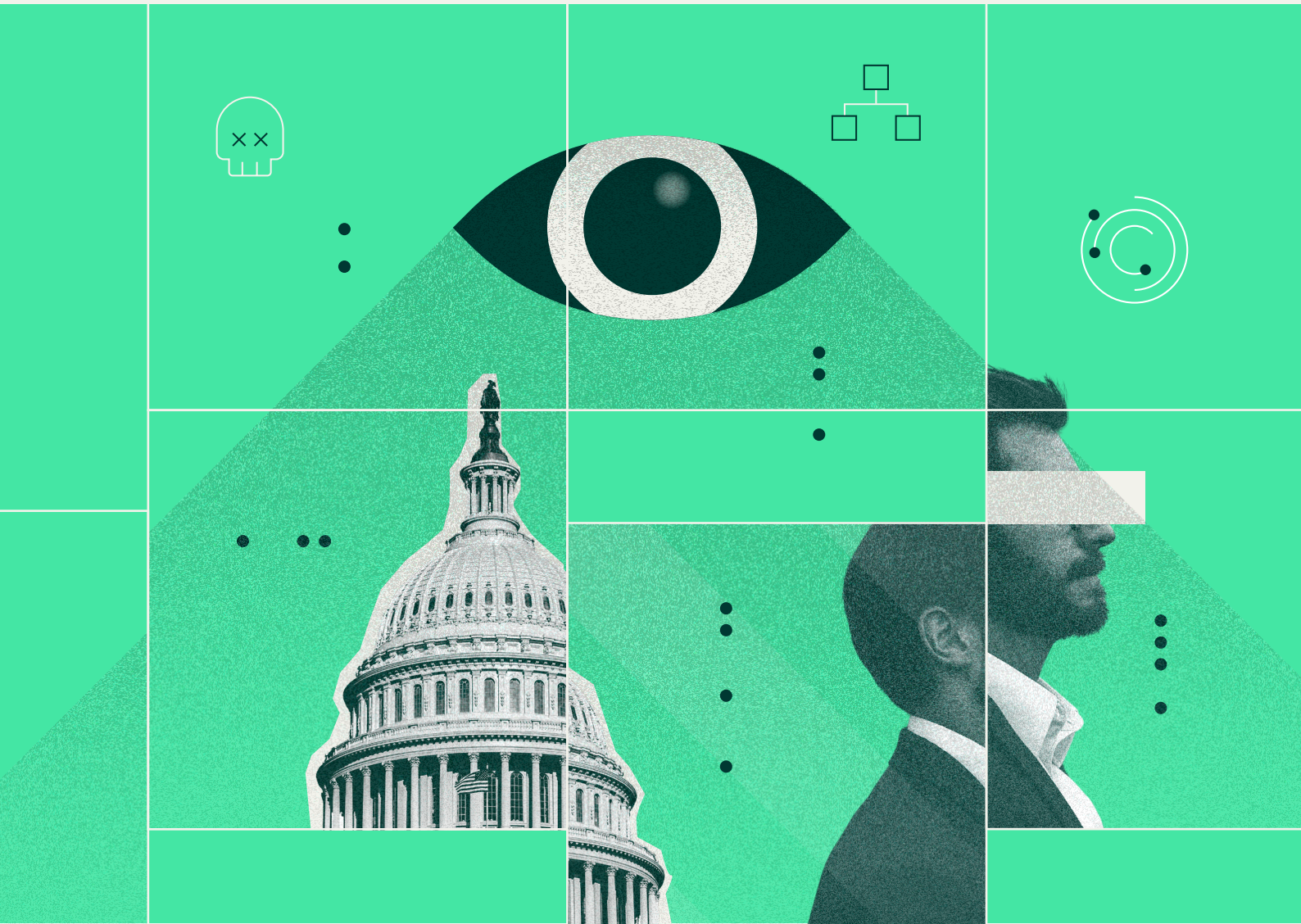
Rubrik Zero Labs

WHITEPAPER

The State of Data Security

The Human Impact of Cybercrime



Contents

This is a story about data and what we stand to lose when it's threatened. It's also a story about people: the people that need data to do their jobs, the criminals who threaten it, and the people who protect it.

In this inaugural Rubrik Zero Labs report, commissioned by Rubrik and conducted by Wakefield Research, we also explore the human impact of securing data through the eyes of the people who do it every day.

Rubrik Zero Labs is on a mission to deliver actionable, vendor-agnostic insights to reduce data security risks. We advance zero trust data security outcomes based on real-world cyber threat assessments and cyber resiliency best practices. Our work focuses on three core pillars:

1

Operationalize Evil Finding
Create proactive, actionable decision points from data-driven observations and trend analysis.

2

Reduce Risk
Work to reduce and limit threat options through research, public advocacy, partnership efforts, and technical changes to core data security technologies or tradecraft.

3

Improve Our Community
Act as a trusted advisor in the data security space through detailed research on security topics, models, and external publications.

"Listen first. Speak last."

Peter Drucker, the father of modern management, said, "Listen first. Speak last." In that spirit, we wanted to kick off Rubrik Zero Labs by listening to the people who prepare for and tackle cybercrime every day.

For a complete, unbiased view, we sought to hear from those outside our client set. To that end, we spoke with more than 1,600 IT and Security leaders, half of which are CIOs and CISOs, from 10 countries on how they view the state of data security. We then asked some of the brightest minds in cybersecurity about what we uncovered and what organizations can do to better secure their data. See the data and the perspectives below.

1,600+
IT and Security leaders

819
CIOs and CISOs

10
Countries Worldwide

Breakdown of Respondents

The global survey was commissioned by Rubrik and conducted by Wakefield Research among 1,625 IT and Security decision makers (Directors, VPs, CIOs and CISOs) at companies of 500 or more employees. The research was conducted in the US, UK, France, Germany, Italy, Netherlands, Japan, Australia, Singapore, and India, between July 18th and July 27th, 2022.

Job level	241 VP	565 Director	408 CISO	411 CIO
Region	500 US	625 EMEA	500 APAC	
Company size	366 2500+	505 1000-2499	754 500-999	

1.0
The Landscape

1.1
Cyberattacks Continue to Surge in Volume and Impact

1.2
Organizations Are Losing Confidence in Their Ability to Withstand Attacks

1.3
Known Threats Remain the Largest Challenge

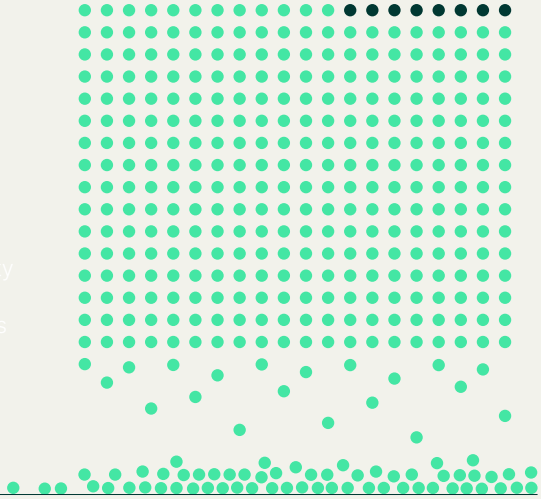
1.1

Cyberattacks Continue to Surge in Volume and Impact

Despite decades of focus and investment in cybersecurity, the news remains the same: Cyber threats aren't letting up. In fact, they're getting worse.

98%

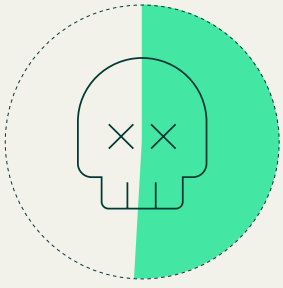
of the 1,600+ IT and Security leaders stated a cyberattack reached their level of awareness within the last year.



On average, IT and Security leaders were made aware of attacks 47 times in the last year

52%

of respondents suffered a data breach.



51%

dealt with ransomware in this same timeframe.

> Intrusions are no longer the sole purview of small, internal teams. Senior leaders, entire organizations, and the larger public are all now aware and impacted by these events.

1.2

Organizations Are Losing Confidence in Their Ability to Withstand Attacks

Both IT and Security leaders as well as organizational leadership appear to doubt their ability to combat threats as the attack surface widens, cybercriminals get more sophisticated, and news feeds constantly highlight the newest hack.

33%

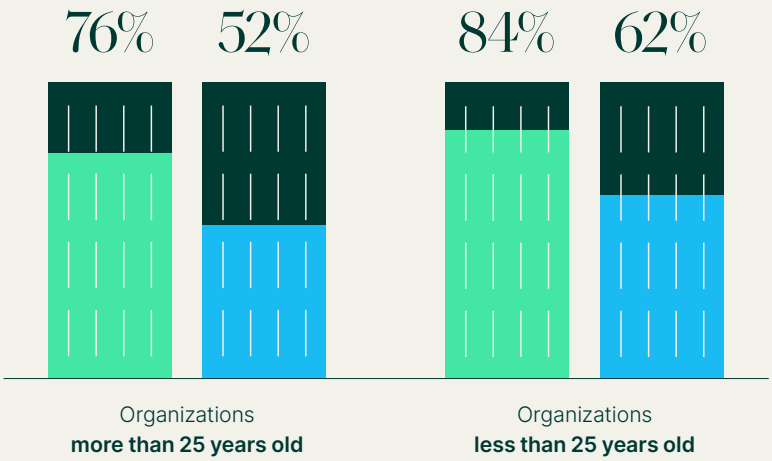
of IT and security leaders believe that their board and executive leadership have little to no confidence in the organization's ability to recover critical data and business applications in the event of a cyberattack.

92%

of IT and security leaders are concerned they won't be able to maintain business continuity if they experience a cyberattack.

When faced with ransomware, respondents said:

- They'd consider paying
- They are extremely or very likely to pay



How confident is your board/executive leadership in the organizational ability to recover critical data and business applications in the event of a cyberattack?

27%

Completely Confident

40%

Usually confident but occasional scrutiny

33%

Little or no confidence

1.3

Known Threats Remain the Largest Challenge

Although zero-day attacks receive much of the cybersecurity industry's attention, only about a third of respondents reported experiencing such an attack in the last year and few see it as their top threat in the coming year.

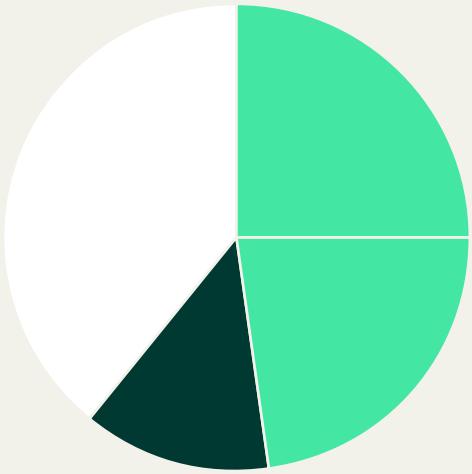
Only 39%

of cyberattacks at the IT and security leader level involved a zero-day exploit in the last year, meaning 2/3 of events leveraged well-known vulnerabilities.

11%

of IT and security leaders said they hadn't adequately addressed vulnerabilities from previous events.

48% of IT and security leaders see the top threat for next year as:



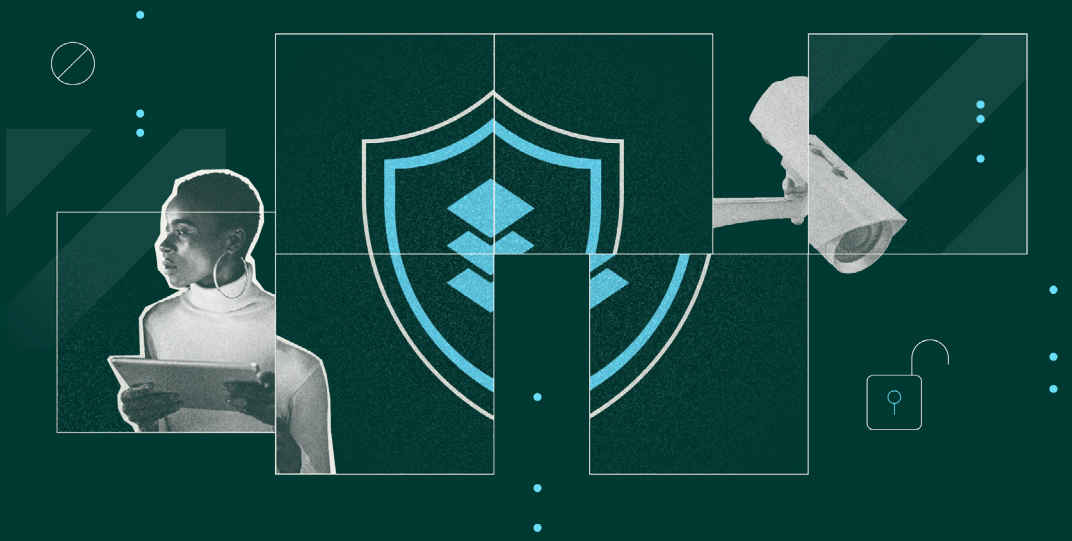
25%
Data breaches

23%
Ransomware events

compared to only
13%
Zero-day exploits

"The combination of cyberattacks rising in number and prominence, emerging threats, and challenges resolving known issues place significant demand on IT and Security personnel.

2.0 The Reality



2.1 IT and Security Leaders Still Need Essential Resources to Secure Their Data

2.2 The Weight of Cybercrime Is Taking Its Toll

2.3 Leaders Struggle to Fully Execute Security Strategies

2.1

IT and Security Leaders Still Need Essential Resources to Secure Their Data

The cybersecurity industry has faced a well-documented talent shortage for years. Open cybersecurity jobs grew by 350% from 1 million openings in 2013 to 3.5 million in 2021, according to Cybersecurity Ventures. Rubrik Zero Labs research respondents unsurprisingly placed talent as their top challenge to protecting their organizations, followed by tools, budget, and C-level or board support.

What are the top five challenges to securing your organization from cyberattacks?

1. Insufficient talent in IT or SecOps teams
2. Lack of cybersecurity tools and solutions in place
3. Insufficient budget for data security
4. Lack of data security prioritization from C-level/board
5. Disagreement between different teams in how to protect against cyberattacks

Historically...

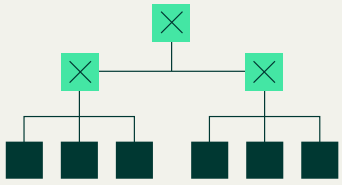
resource shortages are more pronounced at smaller organizations. Smaller entities have the additional burden of fighting all the same threats, but with fewer people and limited budgets.

2.2 The Weight of Cybercrime Is Taking Its Toll

Years of increasing pressure combined with a lack of resources appear to have taken a toll on not only IT and Security leaders and their teams, but across organizations as a whole.

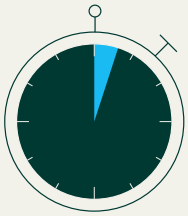
96%

of the IT and Security leaders reported a significant emotional or psychological impact ranging from worries over job security to their colleagues losing trust in them or their organization.



36%

of organizations in our study dealt with a leadership change in the last year due to a cyberattack and its follow-on response.



Only 5%

of organizations were able to return to business continuity or normal operations within one hour of discovering a cyberattack.

96% of respondent organizations experienced negative consequences as a result of a cyberattack. What impacts did your organization experience as a result of cyberattack?

42%	41%	40%	36%	5%
Negative press and / or reputational damage	Loss of customers	Lost revenue	Leadership was forced to change	Negative impact of stock

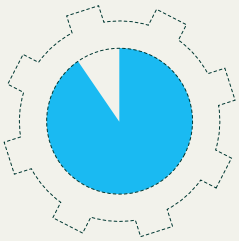
> Human burnout, increasing complexity, and a highly volatile threat landscape are placing significant strain on operations and a high-demand, low-density talent pool. As more intrusions go public, the negative impacts from a single breach are felt across entire organizations.

2.3 Leaders Struggle to Fully Execute Security Strategies

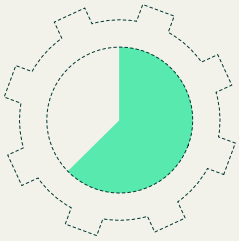
IT and Security leaders have stressed the importance of better aligning IT and SecOps teams to effectively respond to events and make proactive improvements. Industry leaders have also called for public-private sector partnerships to help solve global cybersecurity issues. But Rubrik Zero Labs data shows that making progress on these proposals is more difficult in practice.

31% of leaders surveyed said their IT and SecOps team were either somewhat or not at all aligned when it came to defending their organizations.

Respondents believe public and private sector partnerships are

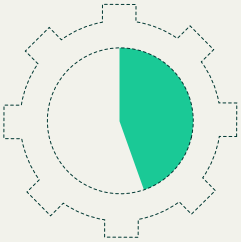


89%
Beneficial



64%
Extremely beneficial

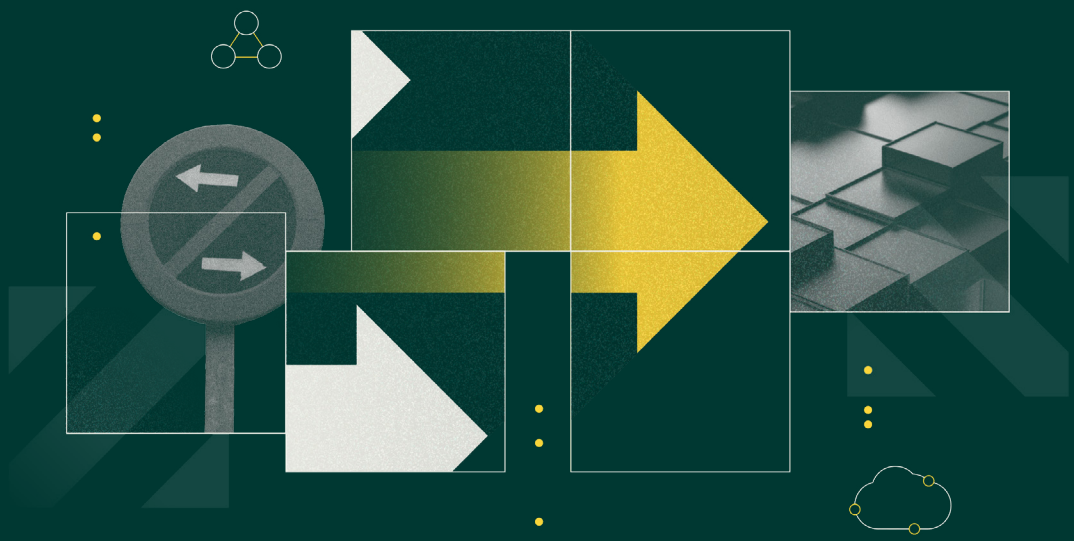
Yet, less than half of those same respondents said they were involved in private-public sector partnerships to tackle cybersecurity.



44%
involved in private-public sector partnerships

> Despite significant effort and investment, organizations continue to struggle with execution. Fundamental architecture and process changes provide the largest returns, but are often challenging to accomplish.

3.0 The Resolution



3.1 What's Next for IT and Security Leaders?

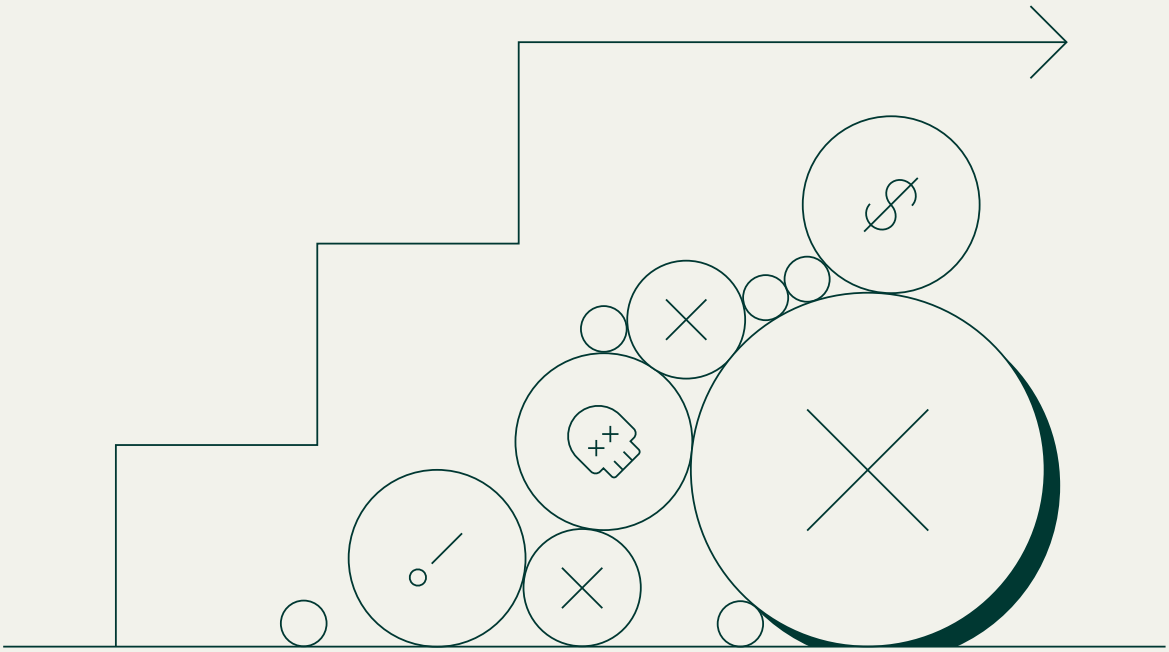
3.2 Best Practices

3.1 What's Next for IT and Security Leaders?

Rubrik Zero Labs research demonstrates IT and Security leaders continue to face a growing list of challenges when it comes to protecting their company's data from cyberattacks.

What, if anything, can they do to overcome the challenges they face?

Leading cybersecurity pioneers and luminaries offer their expert recommendations to address these daunting realities. They've confirmed the gravity of the situation and offered three key best practices that organizations can implement to protect themselves and their data.



3.2 Best Practices

1 Data Breach Readiness Must Withstand *Weekly* Intrusions

IT and Security leaders reported being made aware of 47 cyberattacks against their organization on average last year. That's nearly an attack a week. Since this frequency seems unlikely to slow, these leaders need weekly capacity to address these events. With each incident, organizations should rapidly iterate on both cyber-readiness and crisis-management plans to improve cyber resiliency over time. These improvements will better equip respective teams to restore operations with increased speed and confidence and make each subsequent breach less impactful.

Creating a collaborative process, where each breach effort informs and improves the next, will require participation beyond the IT and Security teams. Legal, HR, and communications teams, to name just a few, will need to devote time and effort into making this type of collaboration work.

> It's no longer a question of if, but when a cyberattack will impact your organization. Preparation can be your secret weapon. Leaders must not only develop a response strategy, but put it into practice so that when an attack happens, you have the right team, solutions, and processes in place to quickly restore your business."
>
> **John W. Thompson**
> Former Microsoft Chairman of the Board, Former Symantec CEO

> Responding to a cyberattack requires collaboration between not only IT and Security teams - but business leaders across all departments. But being prepared for a cyberattack requires not only collaboration, but constant training and practice. Ensuring you have a well thought out data security and recovery plan is a foundational step to enabling business resilience and effective continuity of operations."
>
> **Michael Mestrovich**
> Rubrik CISO, Former CISO of the Central Intelligence Agency (CIA)

3.2 Best Practices

2 Leaders Need to *Ask More* of Their Data

Data is often treated as a passive victim in a cyber event. However, by using data observability technologies, organizations can use data assets themselves to reduce their cyber risk and accelerate incident response times.

Core questions IT and security leaders should ask themselves include:

- How much data is my organization creating and maintaining?
- What data is sensitive or contains personal identifiable information (PII)?
- Where does this data reside?
- Who can access it?
- What data has the greatest business impact?
- Does my organization have the right technologies and processes in place to implement policies based on data volume, importance, sensitivity, and access?
- What supporting systems are critical to maintaining access to this data and in what sequence do they operate?
- How fast can you find answers to your data questions?

These questions may be challenging to answer as employees stay remote and organizations continue moving into hybrid environments. However, they'll also help organizations respond to intrusions and improve resiliency against a wide range of situations, including disaster response, malicious insiders, and accidental data leakage.

> To defend against modern cyberthreats, IT and security leaders must have a deep understanding of their data - who has access to it, where it resides, if it contains sensitive information. Bad actors specialize in capitalizing on blind spots and IT and security teams have a responsibility to their customers to stay a step ahead."
>
> **Asheem Chandna**
> Partner, Greylock Partners

> Protecting your organization and its data comes down to fundamental resiliency. And resiliency comes from securing your data. In the event that a cyberattack makes its way through traditional defenses, if your data is secure, you have the opportunity to quickly recover your business and come out on the other side."
>
> **Shay Reddy**
> CISO, Hanna Andersson

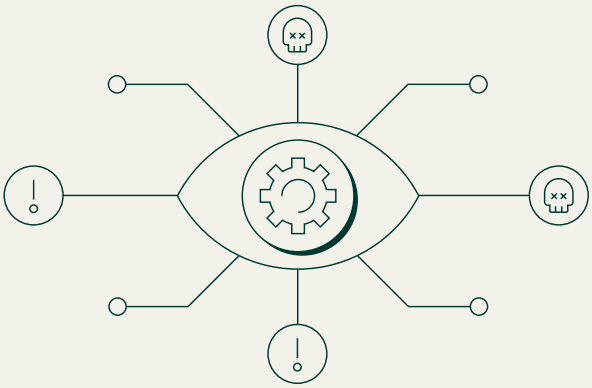
3.2 Best Practices

3 Share Cyber Risk and Threat Insights *Across Teams*

Rubrik Zero Labs data showed the majority of respondents believe they will have fewer resources in the future due to a range of factors, including economic uncertainty, tightening budgets, competing priorities, and larger geopolitical factors.

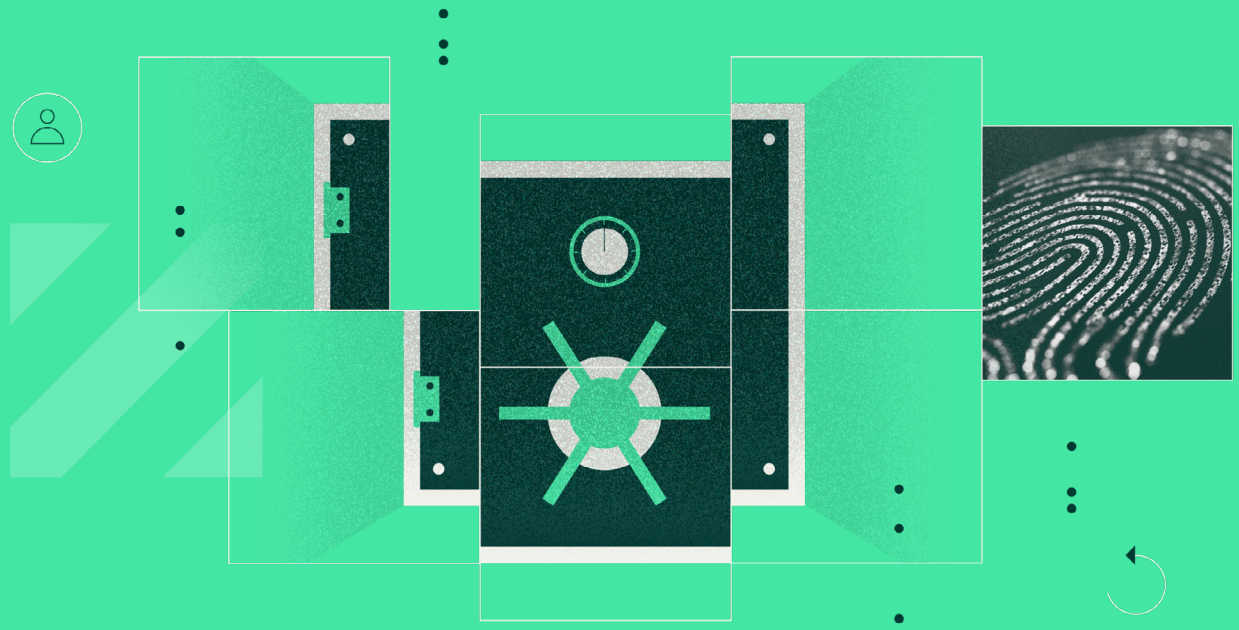
These increasing stressors make it more important than ever for teams to work cross-functionally and operate under a shared view of their data. Improved collaboration facilitated by shared visibility is especially important during a cyber incident, where faster response and recovery is necessary to ensure business continuity, but will also aid in completing routine work.

The more teams using the same tools, process, and visibility across an organization, the better these decisions can be made and applied at scale.



> We often overlook the psychological dimension of cyberattacks and the chaos that tends to follow after discovering an incident. The bad guys sure have figured it out, though, with criminals and state actors alike trying to generate emotional responses when they attack, as evidenced by the increase in criminal extortion efforts and hack and leak campaigns. In the end, IT and security leaders alike tend to take the blame for these cyberattacks. One of the most effective techniques I've seen to prepare for these types of attacks is to accept you're going to have a bad day at some point, and your job is to ensure that it doesn't become a "worse day." This is why we need defenders across the spectrum to come together - sharing best practices, learnings after attacks, simulations, frameworks - so that we're collectively strengthening our defenses and minimizing the psychological impact brought on by an attack."
>
> **Chris Krebs**
> Former Director of CISA and Founding Partner of the Krebs Stamos Group

In Summary



Secure your data in the **fight against cybercrime**

Cybercrime continues to be a persistent threat for many organizations despite the significant time and resources dedicated to protecting their data, applications, and infrastructure. IT and Security leaders need support in the form of executive attention and advocacy, budget, and talent.

However, these resources alone simply won't be enough. Organizations need to leverage their own data assets in the fight against cybercriminals, so they can make their data actionable, keep their data safe and recover more easily, safely, and quickly.

Rubrik Zero Labs