rubrik

BUILDING CYBER RESILIENCE:

Are You on the Right Track?

IT environments and their tightly coupled systems are only getting more complex, leaving them open to failures and cyberattacks. Of the IT and security leaders who experienced a successful ransomware attack in 2024, 86% said that they paid a ransom to recover their data or stop the attack. And of the IT and security leaders that experienced a ransomware attack, 74% said the threat actors were able to harm backup and recovery options.[1] Despite investments in backup and recovery options, organizations are struggling to get back to business when they're attacked, with many resorting to high ransom demands.

Cyber resilience is the ability to anticipate, withstand, and recover from cyberattacks. It's about accepting that incidents will happen and focusing efforts on minimizing impact and enabling rapid recovery. As Gartner predicts, by 2029, 75% of enterprises will use a common solution for backup and recovery of data residing on-premises and in cloud infrastructure, compared with 25% in 2025.[2] Organizations need a way to get unified, holistic visibility into their data to keep all of it protected.

This ebook provides IT and security leaders with a proven framework to:

- Systematically assess your current cyber resilience maturity
- Define your optimal future state
- Execute a prioritized plan to strengthen your security posture across disciplines like data protection, threat analytics, and incident response

Understanding Cyber Resilience

Cyber resilient organizations are able to anticipate, withstand, and recover from cyberattacks. Rather than focusing solely on prevention, cyber resilient organizations put equal emphasis on being able to bounce back quickly when incidents do occur.

One helpful way to think about it is with this simple equation:

Reducing cyber risk, minimizing the impact of incidents, and optimizing recovery capabilities are the key elements that determine an organization's cyber resilience.

1 The State of Data Security in 2025: A Distributed Crisis
2 2025 Gartner® Magic Quadrant™ for Backup and Data Protection Platforms

Reducing cyber risk is about understanding your threat landscape, identifying vulnerabilities, and looking beyond a defense-in-depth approach. But since eliminating risk entirely is impossible, minimizing impact is also critical. This is about containing the blast radius when incidents occur through techniques like segmentation, access control, and encryption.

Enabling rapid recovery is ultimately what determines how quickly you can get the business back up and running. Robust data protection, the ability to surgically extract threat artifacts, and orchestrated recovery workflows are key capabilities here.

Assessing Your Current Cyber Resilience Maturity

So, how do you gauge your organization's current cyber resilience? A maturity model approach provides a helpful framework that includes five levels:

1	2	3	4	5
Unprepared	**Ad Hoc**	**Defined**	**Managed**	**Optimizing**
Completely reactive and ad-hoc	Some plans are in place but are siloed and inconsistent	Plans are documented and aligned across the organization	Processes are measured and controlled	Focus on continuous improvement

To understand where you are in the model, evaluate your current state across the multiple security disciplines that contribute to cyber resilience:

ATTACK LIFECYCLE

Before	During	After
Governance	Sensitive Data Monitoring	Secure Backup
Organizational	Threat and Anomaly Detection	Secure Recovery
Recovery Strategy		Recovery Communication
Sensitive Data Risk Management		Cost Optimization

Starting with these questions will help you identify your strengths and weaknesses. This is an ongoing process that can't be rushed, but you can steadily improve maturity in various areas to meet specific business needs, such as prioritizing sensitive data risks in healthcare, finance, and federal organizations.

Planning Your Cyber Resilience Improvements

With the self-evaluation complete, you can turn to planning your improvements. The key here is to prioritize ruthlessly based on what will have the biggest impact on risk reduction, impact minimization, and recovery optimization.

When moving from one level of maturity to the next, ultimately striving for "Optimizing," consider the incremental steps and milestones to get from your current state to the target and factor in any dependencies.

Consider these key questions to ask yourself:

For Risk Management

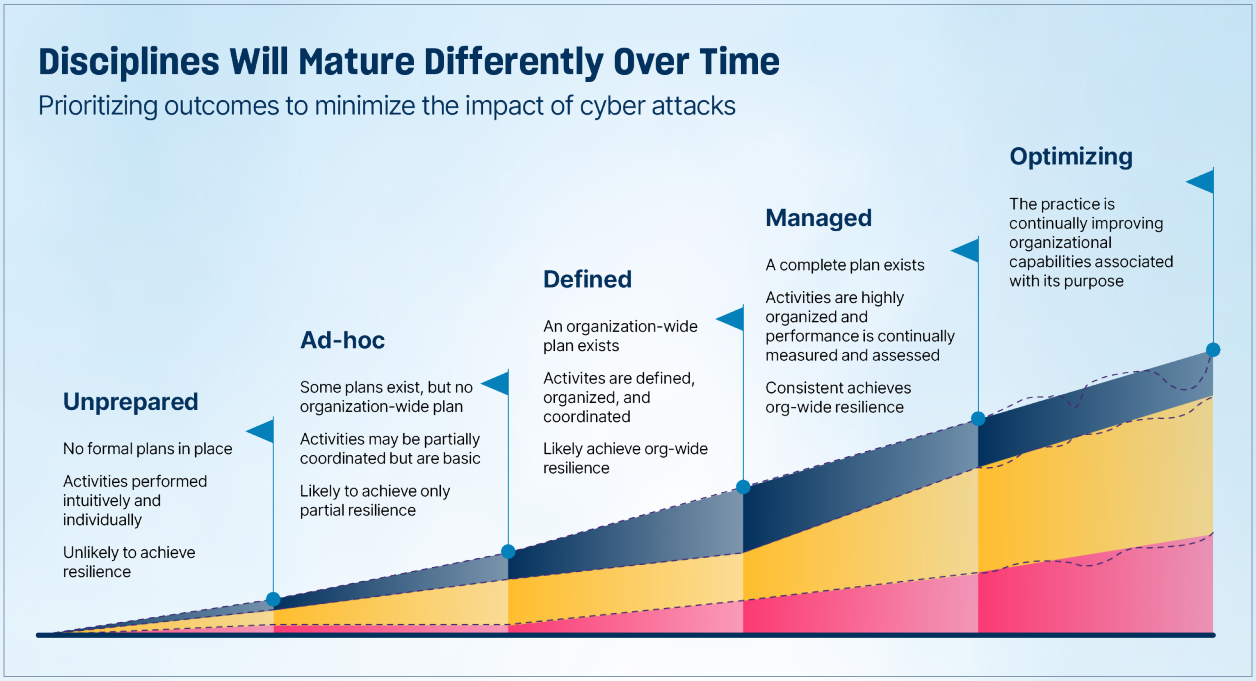
- What are our top risks and threat scenarios?
- Which applications and sensitive data pose the greatest risk?
- What compensating controls or protections should we have in place?

For Impact Minimization

- How can we limit blast radius and propagation?
- Where do we need better segmentation, access control, or encryption?
- How can we reduce the mean time to detect (MTTD) and contain threats?

For Recovery Optimization

- Do we have known-good recovery points for critical data and systems?
- Can we surgically identify and extract threat artifacts?
- Where can we use automation to accelerate recovery?
- Can we eliminate reinfection risks?



The output of this planning process should be a prioritized backlog of improvement initiatives, each with clear owners and timelines.

Executing and Measuring Your Cyber Resilience Plan

With the plan in place, it's all about execution and continuous improvement. An agile, iterative approach works best, with short sprints to implement and test controls, automation, and recovery capabilities.

Ongoing measurement is critical to track progress and prove impact. Some key metrics to track:

- Reduction in incidents and mean time to detect/contain
- Ability to restore to a clean state, free from re-infection risks (Clean cyber RPO)
- Ability to get your business back up and running quickly (Fast cyber RTO)
- Percent of critical systems with air-gapped, immutable backups
- Percent of recovery workflows that are fully automated

Capturing these metrics will help keep the program on track and build buy-in with key stakeholders. Tabletop exercises and purple team tests are also invaluable to stress-test your resilience and identify areas for improvement.

Best Practices for Building Cyber Resilience

1. **Develop a comprehensive incident response plan:**
   - Define roles and responsibilities
   - Establish communication protocols
   - Create playbooks for different types of incidents
   - Regularly test and update the plan

2. **Implement a robust backup and recovery strategy:**
   - Use the 3-2-1 backup rule (3 copies, 2 different media, 1 offsite)
   - Ensure backups are immutable and air-gapped
   - Test recovery processes regularly

3. **Adopt a zero-trust data security model:**
   - Implement least privilege access
   - Use multi-factor authentication
   - Continuously verify and validate all access requests

4. **Enhance threat detection and response capabilities:**
   - Deploy AI-powered threat analytics
   - Implement security orchestration and automated response (SOAR)
   - Conduct regular threat-hunting exercises

5. **Prioritize employee education and awareness:**
   - Provide regular security awareness training
   - Conduct phishing simulations
   - Foster a culture of security consciousness

6. **Implement network segmentation:**
   - Divide the network into smaller, isolated segments
   - Use firewalls and access controls between segments
   - Regularly review and update segmentation policies

7. **Conduct regular risk assessments:**
   - Identify and prioritize critical assets
   - Assess vulnerabilities and threats
   - Develop and implement risk mitigation strategies

8. **Establish a vulnerability management program:**
   - Regularly scan for vulnerabilities
   - Prioritize patching based on risk
   - Implement compensating controls where patching is not possible

9. **Develop and test business continuity plans:**
   - Identify critical business functions
   - Establish recovery time objectives (RTOs) and recovery point objectives (RPOs)
   - Conduct regular tabletop exercises and full-scale drills

10. **Foster collaboration between IT and security teams:**
    - Align objectives and KPIs
    - Establish regular cross-team meetings
    - Encourage knowledge sharing and cross-training

Get on the Right Track

You can't prevent every single cyberattack, so you need to be able to withstand them when they strike — and bounce back with your data intact. Cyber resilience needs to be a priority if you want to do more than skate by after a cyber incident.

As we've explored in this book, building cyber resilience requires a proactive, multi-disciplinary approach. By systematically assessing your current maturity, defining your target state, and prioritizing improvements across disciplines like data protection, threat analytics, and incident response, you can measurably reduce risk, minimize impact, and optimize recovery capabilities.

But technology alone is not enough. Building true cyber resilience also requires the right processes, skills, and culture. By aligning your teams around a shared framework, continuously measuring progress, and cultivating a resilience mindset, you can ensure your organization is prepared to withstand and bounce back from any threat.

So, where will you start?

Take a self-guided tour and see how you can proactively test and automate end-to-end cyber & disaster recovery.

Reach out to a Rubrik professional here to learn what you need to do to make your organization resilient against failures and attacks.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

ebk-building-cyber-resilience / 20250807