

WHITE PAPER

Building cyber resilience in a world of destructive cyberattacks

Assess your business with the Cohesity Destructive Cyberattack Resilience Maturity Model.



TABLE OF CONTENTS

Executive summary	3	Moving from cybersecurity to cyber resilience	9
The new threat and how traditional approaches fall short	4	Enter the clean room	10
The 5 barriers to achieving cyber resilience	6	The importance of staging	12
Traditional BC/DR recovery approaches aren't appropriate for cyberattacks	6	Bringing together IT and Security to deliver cyber resilience	13
Investigation doesn't inform mitigation	6	Introducing the Cohesity Destructive Cyberattack Resilience Maturity Model	14
Security controls may not be available	7		
Security controls may not work after a destructive cyberattack	7		
Security controls may not be trusted	8		

Executive summary

Data is the lifeblood of both commercial and nonprofit organizations. It's an essential component of processes and workflows that have become so reliant on information technology that any attempt to revert to manual "pen-and-paper" processes creates disruptions that can substantially impact an organization's ability to deliver its products or services.

Historically, these disruptions have been the domain of business continuity and disaster recovery, resulting from a small number of well-defined scenarios such as flood, fire, loss of power, misconfiguration, or equipment failure. Today's most likely disruptions are due to destructive cyberattacks.

In this white paper, we'll look at why the traditional approaches IT Operations teams have used to deal with business continuity and disaster recovery scenarios are no longer fit for purpose to handle this new threat. We'll also discuss why the incident response processes Security Operations teams have historically used to deal with nondestructive cyberattacks fall short.

Finally, we'll offer pragmatic steps organizations can take to strengthen their resilience to destructive cyberattacks via the Cohesity Destructive Cyberattack Resilience Maturity Model. Using this model, organizations can assess their resilience maturity today and develop a roadmap to improve their resilience over time.

The new threat and how traditional approaches fall short

While ransomware can trace its roots back to the “AIDS Trojan” released in 1989, it wasn’t until cryptocurrencies appeared some 20 years later that these attacks became easily monetized, leading to the onslaught of attacks we’re experiencing today.

Another type of destructive attack appeared in 2012 when both the Flame and Shamoon wiper malware were discovered. They targeted and destroyed the data related to the interests of Iranian and Saudi Arabian oil companies, respectively. Unlike ransomware attacks, which criminals use for financial gain, these wiper attacks are the work of national state actors or their partisans to harm the interests or economy of another state. With the current state of geopolitics, the world has recently seen a significant increase in wiper attacks.

From the very origins of the discipline of information security to the rise of destructive ransomware attacks, the primary impact organizations faced in this area was data theft. With data theft, unlike with fraud or the theft of a physical good, the organization still has a copy of the data—

and it can use this data to continue delivering products and services to customers. The impacts of these attacks are the secondary losses of reputation damage, potential litigation from partners or the data subjects whose data has been stolen, or regulatory fines.

Today, in the era of destructive cyberattacks such as ransomware and wiper attacks, those secondary losses are joined by a primary loss: the inability of the organization to deliver its products and services. While much of the secondary losses are sunk (meaning their cause originated before the incident occurred by not having appropriate controls in place to prevent the incident), every second spent on response and recovery activities increases the primary losses for the organization. With attacks on the confidentiality of an organization’s data, we had the luxury of being able to tolerate inefficient and ineffective response and recovery processes. With attacks on the integrity or availability of data so critical to the organization, we no longer have that privilege.

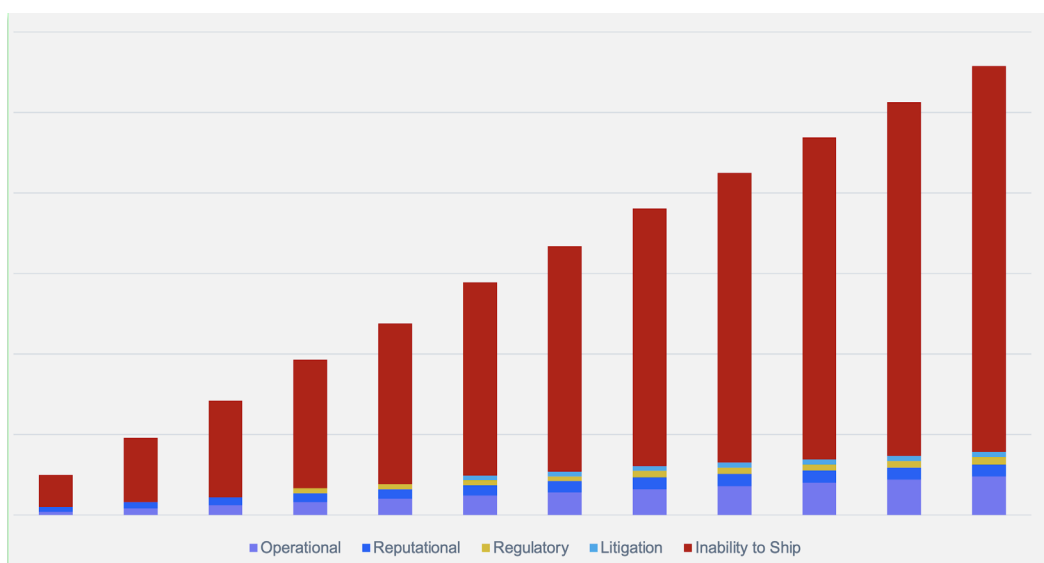


Figure 1: Indicative effects of time over different types of losses

Recent developments in ransomware as a service (RaaS) are only going to make things worse for the defender. Historically, we collectively faced a couple dozen ransomware operators who ran their own infrastructure and conducted the attacks. The number of attacks was limited by the need for ransomware operators to bring together the technical skills required to run their infrastructure.

Many of these operators have found it more profitable to make their ransomware platforms and toolkits available to “affiliates” who don’t require technical skills, just the human resources to conduct the attack. In exchange, the affiliates typically keep 80% of ransoms collected, while the platform operator pockets 20%. RaaS has also let platform operators focus more on innovating their platform’s attack tools to differentiate them from other providers. One result has been the move from using phishing as the primary attack vector to other techniques with higher success ratios, such as weaponizing vulnerabilities in internet connected infrastructure. This can happen within a few days, long before organizations can close the attack surface by patching. Another growing trend is the reuse of credentials stolen in previous attacks.

While we face the growing problem of increased attacks with more severe impacts, most spending on cybersecurity has traditionally been channeled into protection and detection due to the historical focus on attacks against confidentiality. While spending on prevention and detection is critical to prevent the organization from drowning under the barrage of intrusion attempts they see almost daily, it hasn’t been sufficient to deal with

the volume and sophistication of today’s destructive cyberattacks. A quick glance at headlines from the past 12 months shows many organizations with cybersecurity budgets in the tens-of-millions have had their operations significantly disrupted by ransomware. So spending on protection and detection isn’t enough. We keep building our moats wider and our walls taller, but adversaries just build better boats or taller ladders, or they just socially engineer their way right through our castle gates.

Almost all the latest cybersecurity frameworks, such as **NIST Cybersecurity Framework 2.0**, and regulations such as **EU Network and Information Security (NIS2) Directive 2.0** or **EU Digital Operational Resiliency Act (DORA)**, are focused on building resilience: not just the ability to prevent and detect, but also to withstand cyberattacks through responding and recovering, two functions that have been traditionally underinvested in.

The average enterprise has over 130 different cybersecurity tools installed, the vast majority of which have failed to be integrated and operationalized enough to prevent organizations from becoming victims of a cyberattack. Any further investment in prevention and detection is likely to produce only a fractional decrease in cyber risk, while creating more friction with users, less agility for the organization, more alert fatigue, higher licensing costs, and even more security infrastructure to manage. Spending on response and recovery, by contrast, delivers the cyber resilience that these latest frameworks and regulations require and that modern cyberattack threats demand.

The 5 barriers to achieving cyber resilience

Traditional BC/DR recovery approaches aren't appropriate for cyberattacks

One of the largest barriers to moving from cybersecurity to cyber resilience is that in many organizations, the response function is owned by teams overseen by the Chief Information Security Officer (CISO), and the recovery function is owned by the teams overseen by the Chief Information Officer (CIO). These two functions have built these capabilities largely independent of each other because they were originally built to deal with other threats: historically CISOs dealt with data theft attacks, while CIOs dealt with disaster recovery and business continuity (BC/DR). Strategies for BC/DR revolved around a finite number of easily-understood threat scenarios such as flood, fire, earthquake, power loss, equipment failure, or misconfiguration.

The reason organizations with huge cybersecurity budgets and well-established BC/DR programs hit the headlines when they're the victim of ransomware is that these two aspects haven't been adapted to be fit for purpose to withstand destructive cyberattacks. Huge costs and massive customer disruptions are the result.

The CIO's BC/DR plans are designed to cater to a small number of well-defined root causes. Automation and orchestration can play a large part in recovery, and the last snapshot of a system is usually the one that is recovered to.

Contrast this with a destructive cyberattack, where the adversary is actively targeting the backups to render them unavailable, increasing the chances of a successful attack. These adversaries can use any combination of the few hundred MITRE ATT&CK techniques iteratively in any

order to get inside the organization through exploiting vulnerabilities. Once in, they escalate privileges, maintain persistence even after recovery from backup, move laterally around the organization, steal data, and eventually delete or encrypt it.

Organizations that incur the highest costs of a destructive cyberattack are those where the backups have been rendered unusable by the adversary or where attacked systems are recovered without the appropriate remedial steps to remove the threats and vulnerabilities, causing those same systems to be reinfected within seconds or minutes.

Investigation doesn't inform mitigation

When recovering from destructive cyberattacks, the IT Operations team is reliant on the Security Operations team to understand what steps need to be taken to prevent reinfection and reattack. The Security Operations team's investigation uncovers:

- Which vulnerabilities the adversary exploited so IT Operations can patch them before systems are returned to production
- Which malicious accounts and authentication providers to remove from systems
- Which emails are languishing in user inboxes waiting to be clicked again
- What persistence mechanisms reside in changed configuration files and need removal
- Whether the adversary has swapped out any binaries or libraries with malicious ones
- Whether there have been changes to registries or domain forests

- Which controls failed to stop or detect the attack so they can be bolstered to prevent a recurrence
- Any other artifacts of the attack that will need to be removed from the recovered system

Also, as LOL (“living off the land”) attacks are becoming more prevalent, the very tools used to administer the environment are being used against it. How is recovery impacted when PowerShell or SSH are unavailable?

When acting in isolation, the CIO may promise a Recovery Time Objective (RTO) that’s simply a factor of the speed of disk, pipe, and recovery software, independent of the time that the containment, investigation, and eradication steps of the response stage will take. It’s only when an incident happens that an organization learns the harsh lesson that they either need to add the unexpected timeframe for response, or plow ahead without it and undertake multiple iterations of recovery, each adding to the RTO timescale. Otherwise they’ll get reinfected almost immediately. The CIO and CISO need to work together to set realistic expectations with the board and senior executives around achievable RTOs that allow for both response and recovery to occur.

Security controls may not be available

The CISO may have built much of their capability around the data theft scenarios. The organization may have made assumptions about the availability of core IT, Security, and even building facility functions that may not be functional after the attack. In one actual instance, door

access control systems were wiped, preventing physical access to the buildings and rooms needed to even start the response—and Voice-and-IP and email systems were impacted too, preventing communication with insurers, business partners, regulators, law enforcement, and the press. (The press had to use LinkedIn to reach out to the organization’s employees to find out what was happening. They discovered the employees themselves were unaware of what was happening since no one could communicate with them either. Negative press reports ensued.)

BC/DR priorities often focus on critical business applications first because they’ve been drawn up by the IT Operations team working with the business units in isolation of security. But it’s critical to recover a trusted Minimum Viable Response Capability (MiViRC) so IT and Security Operations can work collaboratively with their internal and external stakeholders to manage the incident.

Security controls may not work after a destructive cyberattack

In almost every cyber incident response framework, whether the **SANS Institute Six Step Incident Response Lifecycle** or **NIST SP800-61r2 Computer Security Incident Handling Guide**, the containment stage is critical to preventing the spread of attacks like ransomware and wipers. The challenge is we have become reliant on access to the end point for investigation, eradication, and recovery. Remote forensics imaging and end-point security controls such as **End-Point Detection & Response (EDR)** and **eXtended Detection & Response (XDR)** are commonplace in today’s security arsenal.

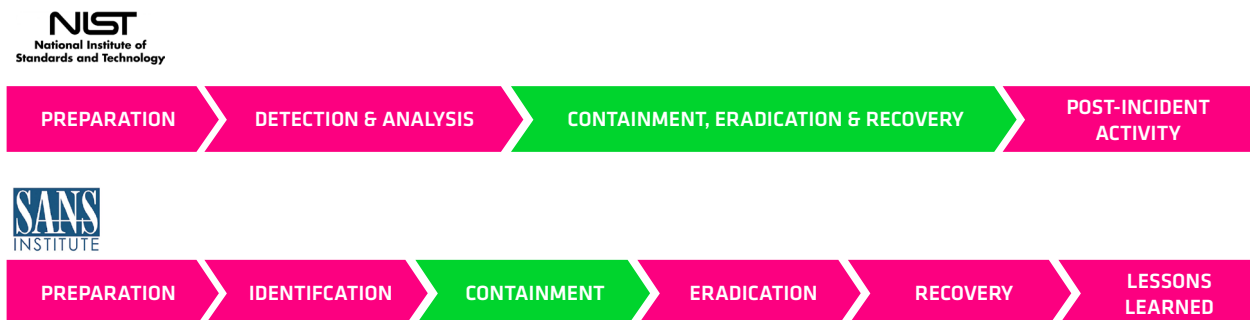


Figure 2: Containment is a part of incident response best practice, but can impede security tooling

Security controls may not be trusted

The MITRE ATT&CK Framework—the de facto standard for analyzing adversary behavior in a cyberattack—has 14 tactics to describe the end-to-end steps an attacker takes. The “Defense Evasion” tactic describes the ways an adversary can circumvent security controls. ***Note that this particular tactic has 42 techniques under it, more than any other.*** Not protecting your backups, and a total reliance on detective security controls that sit on an end-point are subject to compromise. This, in turn, can blind an organization to ongoing ransomware and wiper attacks and leave it unable to recover.

In summary, many organizations plan to have the CIO’s team use traditional BC/DR processes and technology in response to a destructive cyberattack, if the backup itself hasn’t been targeted. The CIO’s team can’t move on to recovery until the CISO’s team has both investigated the incident and established the required remedial actions or risk of reinfection. At the same time, the CISO’s team may not have considered the impact such an attack will have on their ability to perform their response functions—and may be reliant on the CIO’s team to recover their response capability.

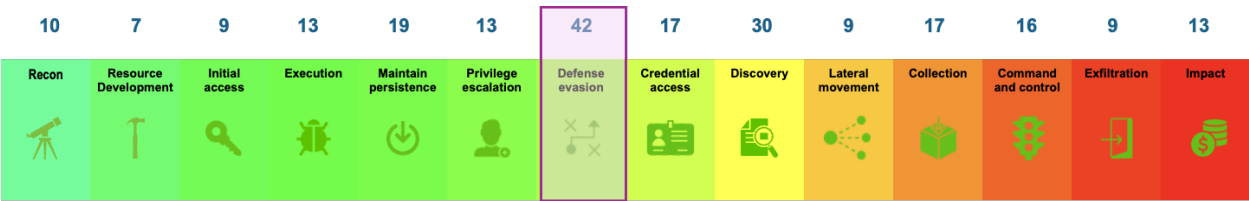


Figure 3: Defense Evasion has the highest number of ATT&CK Techniques of all 14 tactics

Moving from cybersecurity to cyber resilience

Almost all retained incident response companies that deal with these types of incidents daily know that the key to minimizing the achievable RTO in destructive cyberattacks is to establish isolated response and recovery environments. These organizations have to work with customers in the post-incident chaos to establish these environments, but they are the key to bringing systems back up while minimizing the chances of a successful reattack.

Due to their background in catering to traditional BC/DR scenarios, some data management vendors offer isolated environments focused only on the recovery needs of the IT Operations team, forgetting the intrinsic relationship between response and recovery needed to deliver cyber resilience.

By not dealing with the root causes of the incident, there can be significant delays in bringing systems back into production due to having to perform repeated recoveries after reattack. These repeated recovery attempts, each taking the RTO promised to the business, cause the

business to sustain long outages way beyond those the organization considered tolerable when establishing their recovery plans.

Cohesity takes the view that the response needs of the Security Operations team are as important as the recovery needs of the IT Operations team in reducing impact. Approaches that rush to recovering systems without understanding the nature of the attack don't remove the attack surface or artifacts of the attack. Ongoing attacks will reinfect recovered systems within minutes. Ransomware gangs are increasing their use of "double tap" attacks—where they circle back and reattack organizations they previously hit who refused to pay a ransom. These attackers will take advantage of the same vulnerabilities they used to gain access the first time if they're not closed.

Cohesity has built a single platform with capabilities that can be used by both teams to improve the effectiveness and efficiency of both the response and recovery function.

Enter the clean room

While there are many definitions of a clean room, at Cohesity, we define a clean room as an isolated environment where the Security Operations team can perform the necessary investigatory steps to understand how an attack happened. Building a timeline of the incident allows them to draft a manifest of remedial steps to take at the recovery stage to eradicate the threat and help prevent reoccurrence.

The clean room is typically owned by the Security Operations team. At this investigatory stage, systems aren't being recovered. They're being investigated in isolation, so interdependencies are largely irrelevant. Isolation ensures that known-good security tooling is used to avoid the Defense Evasion (discussed earlier), that the adversary can't observe or disrupt response actions, and that there's no risk that machines that have already been recovered will be reinfected by systems inside the clean room.

The clean room is a part of, and reliant on, a Minimum Viable Response Capability (MiViRC) that Cohesity can establish in minutes. Building trusted, known-good infrastructure supports the collaboration, communication, and other workflows of the response and recovery process. Restoring security operations tooling to a known-good state that's used within an isolated environment helps the organization circumvent the many evasion techniques adversaries use.

Cohesity also provides a number of native capabilities to support the needs of the Security Operations Team in the clean room. Thanks to the threat hunting capabilities in [Cohesity DataHawk](#), incident responders have a curated feed of over 170,000 Indicators of Compromise (IoCs) used by ransomware operators across the MITRE ATT&CK Framework. This helps organizations understand the techniques adversaries use across the entire lifecycle of the attack.

The curated feed can be augmented by the customer's own threat intelligence feeds or those provided by a third party. Artifacts found on systems by the customer's Security Operations team during the forensics stage can be fed back into Cohesity to hunt for additional systems that have been impacted. These systems can then be brought into the scope of the investigation.

As threat hunting with Cohesity isn't reliant on an end-point agent, it isn't susceptible to the defense evasion techniques used against XDR and EDR systems. It's also completely passive, so it can't be detected or disrupted by the adversary. As threat hunting with Cohesity is powered by the backup, it will continue to function even when the organization has isolated hosts and networks for containment. Plus, the retention period for backups in many organizations is longer than the logs security solutions typically hold. This gives organizations a chance to detect the activities of nation-state actors who are conducting low-and-slow attacks, such as prepositioned wiper attacks with extended dwell times.

In traditional digital forensics, investigators had to rely on a single forensic image taken post event, forming hypotheses about how a system landed in a particular end-state. With [Cohesity DataProtect](#), forensics investigators are now free to time-travel across the entire incident timeline, loading images of a file system state in seconds. Today's investigators can use their tooling to compare file systems to rapidly identify deltas in configurations and find persistence mechanisms and malicious accounts. Or they can extract binaries for detonation in sandboxes, producing more IoCs that can be fed into DataHawk's threat hunting capability.

While many organizations may have a good handle on the regulatory implications of data held in their structured data stores (such as databases), most have a plethora of unstructured data that contains regulated and other

sensitive data. It's notoriously difficult to understand this data since it can be spread so widely across the organization—and in the event of a destructive cyberattack it's likely to have been encrypted or deleted. The data classification capability within Cohesity DataHawk uses advanced AI/ML-based detections to locate and classify this diaspora of regulated data directly from the backups, easing compliance with regulatory requirements to notify the regulator and data subjects of any confidential compromise of data.

Cohesity established the [Data Security Alliance](#) to bring the context of an organization's data to the existing tools used by the Security Operations team. In an age of cloud, containers, and hypervisors—where infrastructure can be instantiated in seconds—it's the data that can't

be easily replaced. It's also the data that has compliance regulations and data that the adversary is ultimately aiming to steal, encrypt, or wipe. By building relationships with leading security vendors, such as Palo Alto Networks, Cisco, CrowdStrike, ServiceNow, Tenable, Qualys, BigID, Okta, Securonix, CyberArk, and Zscaler, as well as organizations experienced in delivering security-related professional services such as Mandiant and TCS, Cohesity is at the leading edge of driving innovation in how data-context can revolutionize cyber response and recovery—and help organizations get more value out of existing cybersecurity spend.

The importance of staging

A staging room is a recovery environment typically owned by IT Operations into which systems are either rapidly rebuilt from known good sources, or recovered and cleaned. They're where the threat mitigation steps defined by the Security Operations team are undertaken. They're also where interdependencies between individual hosts are satisfied before the functional capability being restored is tested to make sure that recovery and mitigation steps haven't introduced problems back into production. The mitigated systems are then backed up one final time, providing a baseline in case something slipped through the net, so response actions don't have to start at square one.

[Cohesity SmartFiles](#) provides a capability to store known-good installation media on immutable storage, helping ensure it's beyond the reach of the adversary. It can then be rapidly mounted on Windows and Linux systems, allowing IT orchestration or scripting tools to rebuild systems. Golden master copies of systems can be backed up by Cohesity DataProtect and cloned, allowing configurations and data from snapshots across the timeline to be restored as directed by the findings of the Security Operation team's investigation.

- Take proactive measures to reduce the impact of an attack so businesses have trusted resources available when they need them.
 - Destructive cyber attacks target an organization's ability to respond and recover.
 - Endpoint security controls can't always be trusted post incident.
 - Until you know how you were attacked and close the vulnerabilities and bolster controls you will be vulnerable to re-attack.
 - Recovery without closing the vulnerabilities, adding additional preventive and defective controls and the eradication of persistence mechanisms and other attack artefacts leaves you open to re-attack.
 - Mitigations and recovery may have caused functional problems.
- ^a Increase your incident response readiness with a hardened platform, adherence to the 3-2-1 backup rule, and clear communication protocols.
- ^a Traditional security tools struggle to function when an organization has isolated systems in response to ransomware or wipers.



Figure 4: Incident timeline showing the progression from attack to recovery

Bringing together IT and Security to deliver cyber resilience

Bringing together the response workflows, teams, and technology used by the Security Operations team with the recovery workflows, teams, and technology used by the IT Operations team is key to strengthening cyber resilience. Focusing myopically on these functions in isolation will only result in increased impacts when a cyber event occurs.

Cohesity's approach to providing a single platform for both teams speeds the response actions of the Security Operations team while integrating with their incumbent security tooling. This helps improve the efficiency and effectiveness of both response and recovery, strengthening resilience and reducing impacts.

How to use a clean room for incident response

Many organizations lack the proper environment to quickly investigate incidents, and ensure they're not reinfesting systems when restoring their data.

Watch our on-demand webinar for practical details on creating an incident response strategy that strengthens your organization's preparedness and response capabilities—without introducing further risk.

[Watch the webinar](#)

Introducing the Cohesity Destructive Cyberattack Resilience Maturity Model

In this paper, we discuss several proven concepts to improve cyber resilience. The next logical step is to assess your resilience capabilities and understand how (and where) you can improve.

To this end, we present the **Cohesity Destructive Cyberattack Resilience Maturity Model**.

This maturity model is designed to help organizations develop their resilience to destructive cyberattacks such as ransomware and wiper attacks. The model sets clear

benchmarks and features a structured roadmap to guide organizations as they work to achieve effective and efficient operations that are resilient to cyberattacks.

The Cohesity model is aligned with the most common cybersecurity response and recovery frameworks such as [SANS Institute 6 Step Incident Response Process](#), [RE&CT framework](#), [MITRE D3FEND](#), and [NIST SP800-61 Computer Security Incident Handling Guide](#), allowing organizations a path to adopt industry-wide best practices.

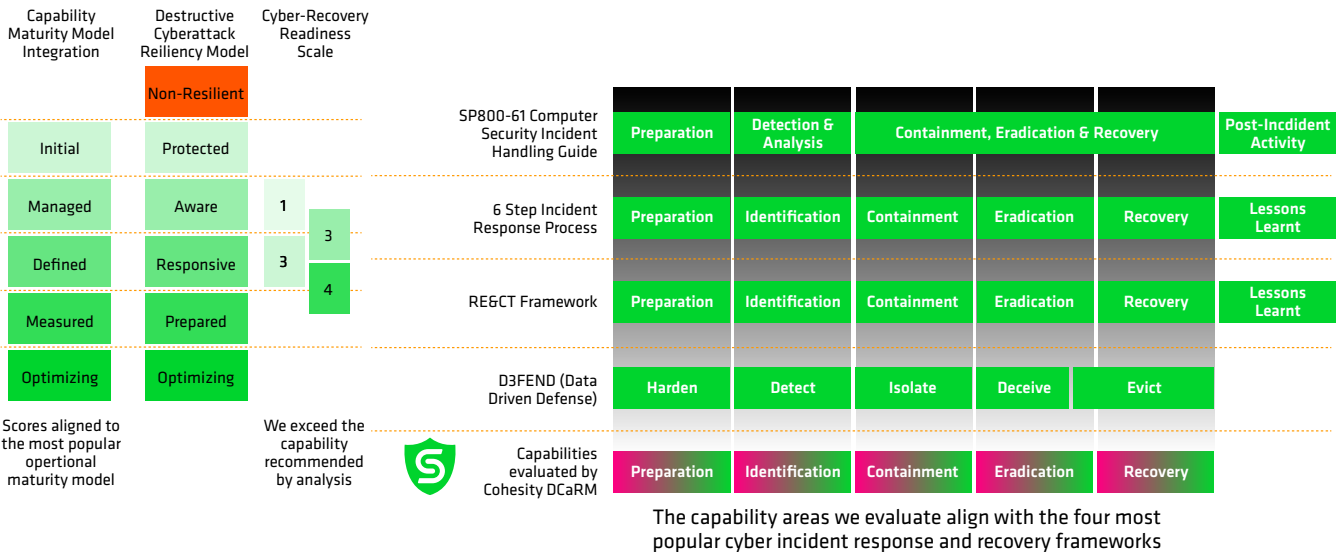


Figure 5: Indicative alignment of the Cohesity Destructive Cyberattack Resilience Maturity Model with common response and recovery frameworks

The maturity model allows organizations to assess their operational capability across the five stages required to achieve cyber resilience:

- 1. Preparing for an incident
- 2. Identifying and investigating the attack
- 3. Containing the spread of the attack

- 4. Eradicating threats and reducing attack surface to prevent future attacks
- 5. Recovering systems to a secure state

The levels of maturity in the model are depicted in the table below:

Maturity Level	Description
Non-Resilient	The organization lacks the resilience to withstand a destructive cyberattack without significant impact to the delivery of its products and services.
Recoverable	The organization has built disaster recovery and business continuity capabilities, but these may be subject to attack by adversaries and lack appropriate investigatory and remediation stages to prevent reinfection or reattack.
Strengthened	The organization has protected its ability to recover from attacks by adversaries.
Aware	The organization has the ability to hunt for the early stages of a destructive cyberattack that can't be evaded and isn't impacted by the containment stage of incident response. A shared responsibility model between IT and Security Operations to deal with incidents has also been developed.
Responsive	<p>The organization has the ability to recover the tools needed to drive incident response and communications with stakeholders to a trusted state, and has isolated environments that allow incident investigation, eradication of threats, and systems testing prior to recovery to production.</p> <p>The organization drives continuous improvements by conducting end-to-end attack drills of diverse attack situations, building muscle memory in incident responders to deal with any future situation, optimizing processes, and looking for opportunities for automation to increase effectiveness and efficiency. The organization is able to rapidly recover the infrastructure and resources needed to manage and respond to the incident should they be impacted by the attack.</p>
Optimizing	The organization has metrics and telemetry to drive continuous optimization of processes, people, and technology. Proactive discovery and classification of data ensures end-to-end governance and regulatory compliance. There is a capability to not just recover systems, but to rapidly rebuild infrastructure to a trusted state. Incident investigation, infrastructure rebuilding, and data recovery are optimized so these tasks can be done in parallel.

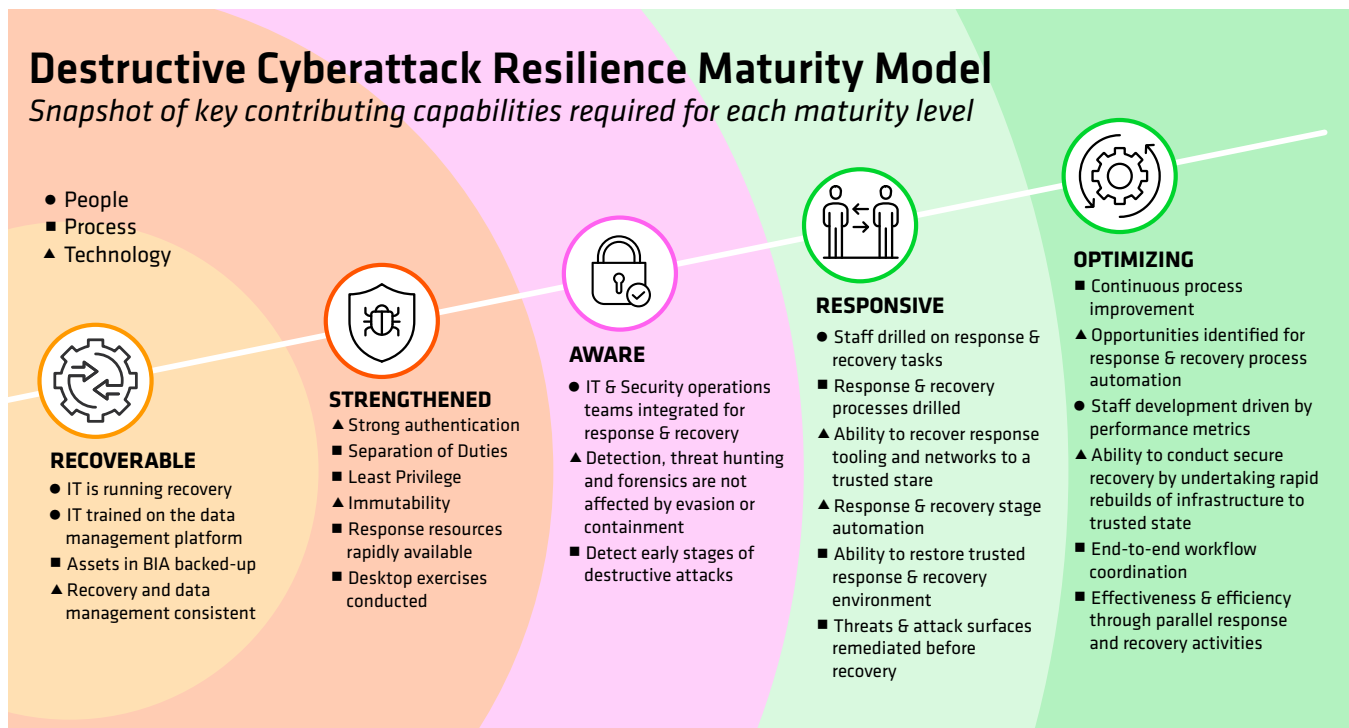


Figure 6: Snapshot of key contributing capabilities for each maturity level of the Cohesity Destructive Cyberattack Resilience Maturity Model

The Cohesity Destructive Cyberattack Resilience Maturity Model provides a vendor-agnostic roadmap. This approach allows its users to align with best practice response and recovery frameworks while achieving a state of cyber resilience and developing appropriate governance, people, and processes. The roadmap ensures that technology is supporting and optimizing operational outcomes, not driving them.

Let's look at the levels of maturity in a greater detail:

- **Recoverable:** An organization that is at this level may have a mature level of disaster recovery and business continuity. They have conducted appropriate business impact assessments to identify critical services and the infrastructure that supports them, and created Recovery Point and Time Objectives (RPO/RTOs). This organization will lack the needed protections on its data management platform to protect them from attack by an adversary. They will also typically treat a destructive cyber incident as a traditional disaster recovery and business continuity scenario, without taking into consideration the complicating factors of a cyberattack. At this level, a close working relationship between IT and Security

Operations to deal with cyber incidents is lacking.

- **Strengthened:** At this level, the organization has recognized that it will be attacked by an adversary, and has put protections in place to mitigate the impact of this inevitability. It has implemented security principles such as least privilege access, immutability (to prevent the malicious changing or deletion of backups), separation of duties (to prevent a rogue or compromised administrator from making damaging changes), and vaulting (to put the ability to recover beyond the reach of the adversary). Vaulting also helps the organization adhere to secure backup conventions like the 3-2-1 principle.
- **Aware:** Organizations at this level have adopted a well-defined shared responsibility model between IT and Security Operations. They have the ability to hunt for threats, and conduct digital forensics even when adversaries evade endpoint security systems. Further, the organization can continue threat hunting during containment, when hosts and networks are isolated. Threat feeds are used, but are often stale, and don't include regular updates to reflect the latest confirmed

threats from ransomware-as-a-service platforms and vulnerabilities. Organizations also lack a defence-in-depth model for hunting for those early stages of an attack before systems are impacted .

- **Responsive:** At this level, organizations take the incident investigation and threat remediation steps necessary before systems are recovered back into production to prevent reattack or reinfection from the same actor. Isolated investigation and remediation environments are in place to achieve the requirements of containment. This level of maturity also introduces continual improvement and practice, so the processes, people, and technology required to respond and securely recover from an incident are ready ahead of time. (You don't want the first time you SOC analysts, incident responders, and senior executives to experience a ransomware or wiper attack to be the one where your data is being held to ransomware or all systems in the business have been wiped. Tabletop exercises are useful, but they don't test the end-to-end workflow, skills, and technology required in a real scenario.)

Organizations also conduct realistic attack scenarios that prepare all components required for cyber resilience. No two incidents are ever the same; by varying aspects of the drills the organisation is better able to optimize processes. The organization regularly looks for opportunities for automation, and to build muscle memory in staff.

Finally, organizations in this stage can rapidly reestablish trust in their networks and security tooling—and have other resources on hand within minutes to start their response activities. They have a reliable way to coordinate, communicate, and investigate the attack in a worse-case scenario. In other words, they're prepared for scenarios

where security controls are evaded, door access systems are down, and there are no CMDB, ticketing systems, email, or voice-over-IP to talk to law enforcement, cyber insurers, the press, regulators, or impacted data subjects.

- **Optimizing:** This level represents the pinnacle of cyber resilience. The organization has taken proactive measures to discover and classify that the data the organization uses can not only be recovered, but that appropriate risk management steps have been taken throughout its lifecycle. Workflows are optimized to align with regulations and impacted data subject notification requirements, so fines are avoided and the organization can comply with DORA, NIS 2, HIPAA, the Prudential Regulatory Authority, and the Security and Exchange Commission as applicable. While the Responsive maturity level seeks opportunities for automation in workflows, Optimizing looks for overall governance, orchestration, and management of the entire end-to-end incident response and recovery process. This maturity level gives senior executives, boards, and stakeholder third-parties confidence that the organization is on the forefront of cyber resilience.

Preparing for and dealing with cyberattacks has made a model like this one critical. These attacks represent the greatest threat to the delivery of products and services by organizations today. Cohesity cybersecurity experts and practitioners with decades of experience in cyber incident response and recovery designed this model so organizations like yours can understand your current capabilities, benchmark your maturity against peers in your industry or geographical area, and have a roadmap for future improvements you can make and measure over time.

About the author

James Blake has over three decades of operational experience in cyber incident response and has built the end-to-end security operations capabilities for more than 30 Fortune / FTSE 100 companies. He has also been involved in the aftermath of hundreds of large scale incidents, including multiple nation-state wiper attacks and dozens of ransomware attacks. He is the Head of Global Cyber Resiliency Strategy at Cohesity.

Learn more at [Cohesity.com](https://www.cohesity.com)

© 2025 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

[cohesity.com](https://www.cohesity.com)

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

2000059-002 EN 4-2025