Building cyber resilience in a world of destructive cyberattacks

COHESITY

COHESITY

Table of Contents

COHESITY

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.

COHESITY

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 malwares 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, in that their cause originates before the incident occurs 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 the data that's the lifeblood of the organization, we no longer have that privilege.

COHESITY

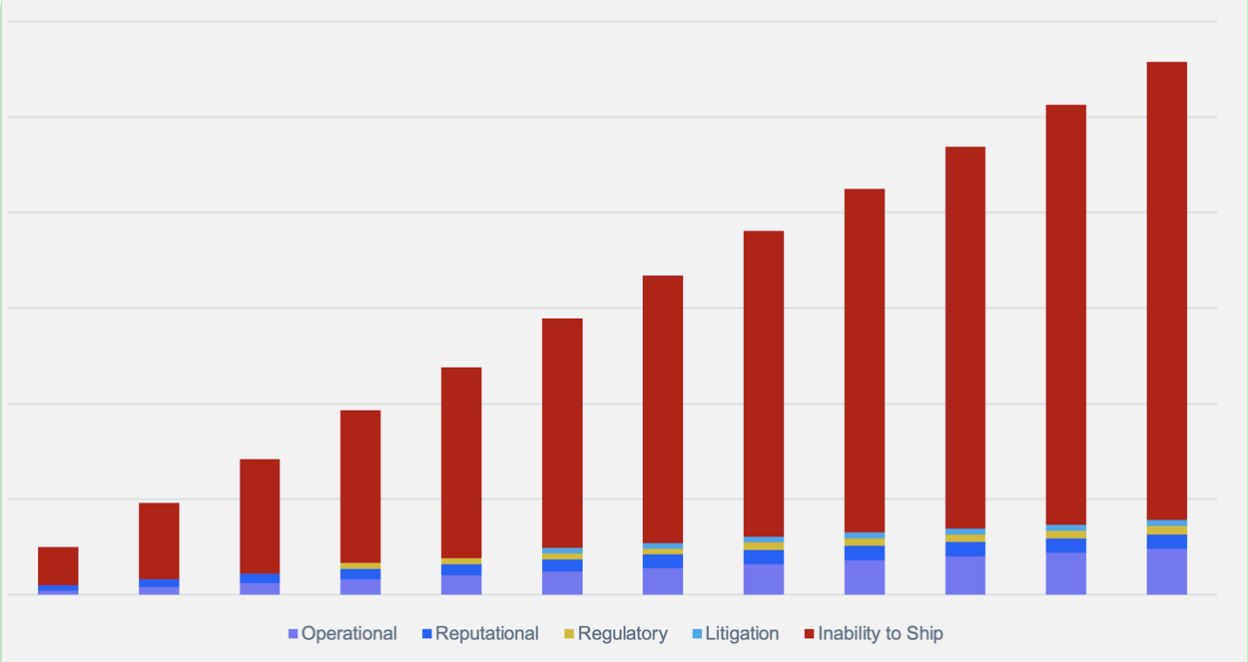

Fig. 1: Indicative effects of time over different types of losses

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 of 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.

COHESITY

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 being reinfected within seconds or minutes.

COHESITY

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 againWhat 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; and
- Any other artefacts 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.

Security controls may not be trusted

In destructive cyberattacks, the MITRE ATT&CK Framework—the de facto standard for describing adversary behavior—14 stages (tactics) are used to describe the end-to-end steps an attacker takes to get tactic 13 (Exfiltration) where data is stolen and tactic 14 (Impact) where it is encrypted or deleted. Out of all 14 tactics, the Defence Evasion tactic that describes the ways an adversary can circumvent security controls has more techniques under it than any other. Not protecting your backups and total reliance on detective security controls that sit on an end-point that is subject to compromise can blind an organization to ongoing ransomware and wiper attacks and leave it unable to recover.

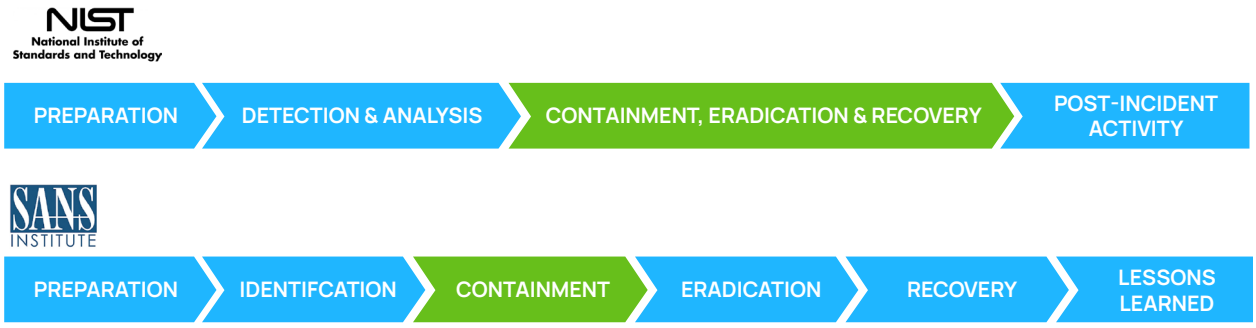

Fig. 2: Containment is a part of incident response best practice, but can impede security tooling

COHESITY

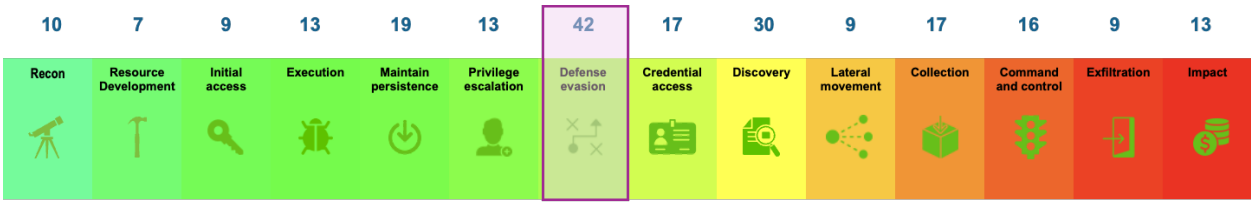

Fig. 3: Defence Evasion has the highest number of ATT&CK Techniques of all 14 tactics

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.

COHESITY

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 artefacts 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 but that 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.

COHESITY

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 Defence 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. Another advantage is that it's 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 provides an opportunity for organizations to detect the activities of nation-state actors who are conducting low-and-slow attacks, such as prepositioned wiper attacks with extended dwell times.

COHESITY

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 withinCohesity 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, 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.

COHESITY

The importance of staging

At Cohesity, 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 Unix 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.

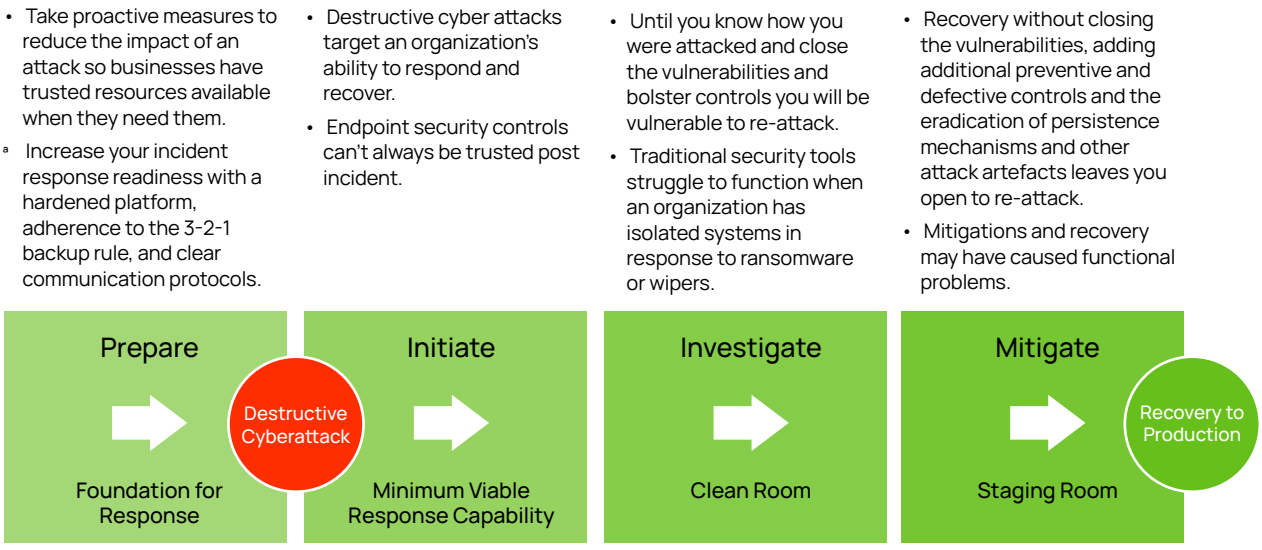

Fig. 4: Incident timeline showing the progression from attack to recovery

COHESITY

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.

Cohesity created the Ransomware Resilience Workshops so senior executives can experience first-hand the decisions they'll be faced with during a cyber incident, along with the likely consequences of their actions. Subject Matter Experts experienced in leading incident response are on hand to provide expert guidance and best practices, along with pragmatic advice for participating organizations.

COHESITY

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.

COHESITY

www.cohesity.com

2000051-002-EN 2-2025