druva

Reducing the Cyber Recovery Timeline

Address Gaps Between Response, Backup & Recovery with Druva's Cyber Resilience Maturity Model

Whitepaper
10/22/2024

v.1.0

Authored by
Rahul Deshmukh,
VP, Product Marketing

In 2024, organizations reported the mean cost to recover from a ransomware attack is

$2.73M

Up from $1.82M in 2023

Source: "The State of Ransomware 2024." Sophos. 2024.

In 2023, cyberattacks cost organizations an average of **$4.45 million per breach**[1]. As businesses increasingly rely on data as a strategic asset, breaches result in financial losses, operational disruptions, and reputational damage, underscoring the urgent need for organizations across industries to prioritize strengthening their cybersecurity strategies.

Although global spending on security and risk management is projected to reach **$215 billion in 2024**[2] — a 14.3% increase from 2023 — cybercriminals continue to exploit system and process vulnerabilities. This threat has transformed data protection from a passive last line of defense to an active player in incident response and recovery (IRR). Organizations have to adjust their strategies to effectively counter sophisticated attacks, especially those targeting critical data and backup systems.

This whitepaper empowers businesses to tackle cyber threats and strengthen incident response using Druva's Cyber Resilience Maturity Model, a framework for assessing readiness and improving cyber resilience. This model, drawing from Druva's extensive customer experience, provides practical guidance and techniques to assess and advance through maturity stages, boosting resilience, data protection, and mitigating risks.

Unseen Obstacles: Navigating Cyber Resiliency Challenges

Cybersecurity tools like XDR, SIEM, and SOAR have been developed to enhance security monitoring, threat detection, and orchestration, but they often fall short in critical areas, including backups. Their perimeter-based approach limits their ability to capture and analyze telemetry data effectively, resulting in insufficient visibility into abnormal behavior within backup environments. This can lead to delayed detection and inadequate response, ultimately compromising the organization's ability to manage and contain cyber threats. To enhance cyber resiliency, organizations must adopt integrated solutions that provide holistic visibility and empower coordinated response across their entire IT environment, including robust protection for their backup systems.

The meantime it took defenders to identify and contain a breach was

258

DAYS

Source: "Cost of a Data Breach Report 2024." IBM. 2024.

[1] "Cost of a Data Breach Report 2023." Ponemon Institute. 2023.
[2] "Forecast Analysis: Information Security and Risk Management, Worldwide." Gartner. 2024.

Despite Advances, Organizations Face Significant Cyber Recovery Challenges

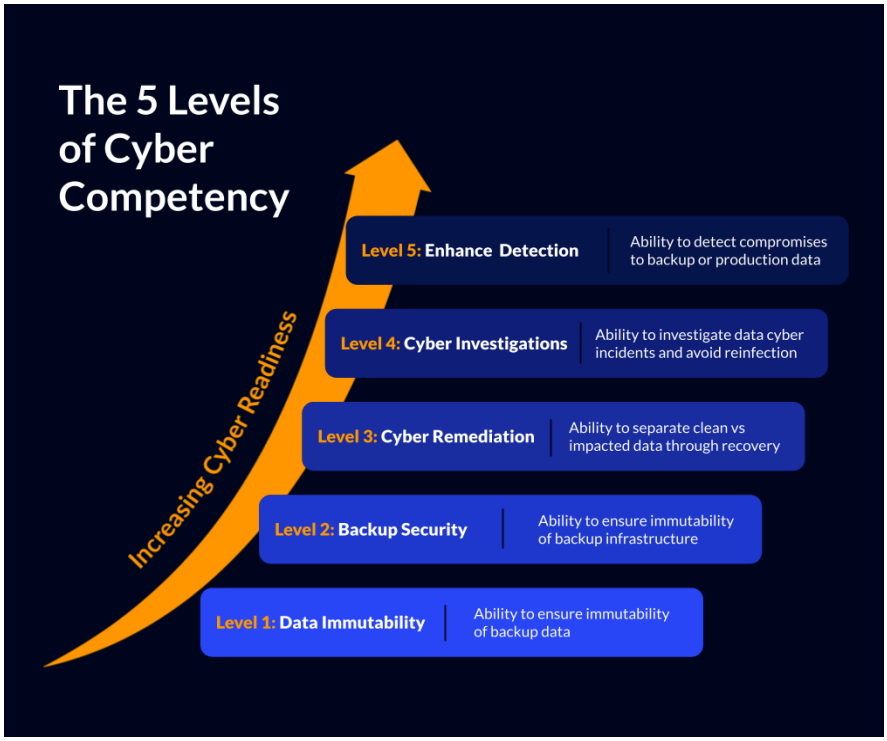
Cyber recovery differs from traditional disaster recovery. With cyber recovery, organizations must identify and separate clean data from potentially infected files, a process complicated by the dwell time of threats that slowly compromise data over time. Without automated tools, organizations face extensive manual efforts to roll back to older copies, resulting in data loss or prolonged downtime. Challenges include:

- **Gaps Between Security and IT**: There's often a void between security and IT operations, which complicates the cyber recovery process. Without clear coordination, understanding what constitutes "clean" data and identifying points of reinfection can become difficult, delaying recovery efforts.
- **Compromised Backups**: In many cases, backups may be compromised by malware, disabled, or rendered inaccessible. This might involve deleted users, changed policies, or injected garbage data, leading to unusable backups or longer recovery times.
- **Determining Clean Data**: Establishing what data is clean and free of malware, encryption, or corruption can be complex. This requires a shared responsibility between security (to identify malware) and IT (to recognize encryption or corruption).
- **Scope and Containment Issues**: Identifying the extent of malware impact and containing it effectively is challenging. Persistence mechanisms in malware, such as Trojans, may allow reentry and re-infection, further complicating containment efforts.
- **Lack of Proactive Detection**: Organizations may lack proactive data-oriented detection, which helps in spotting changes like unauthorized encryption. If threats are not identified early, recovery becomes more reactive, adding delays.
- **Complex Recovery Process**: Cyber recovery isn't linear; as systems are recovered, further investigations may reveal additional compromised systems, requiring additional steps and slowing the process.
- **Ownership and Responsibility Issues**: There can be ambiguity around who is responsible for various aspects of recovery, such as identifying clean data. Shared or unclear responsibilities can lead to delays in addressing these critical areas.

Introducing the Cyber Resilience Maturity Model

To tackle challenges like scope, containment, and reinfection, organizations must prioritize proactive data security alongside existing strategies.

As a leader in cloud data security, Druva uses the five levels of its Cyber Resilience Maturity Model to assess readiness, identify gaps, and create a roadmap for improvement.



Level 1: Data Immutability

Backups serve as the last line of defense in cyber incident recovery, so it's vital to keep backup copies immutable and stored in air-gapped locations. Data immutability ensures availability and integrity, forming the foundation of an organization's cyber resilience. With secure, immutable backups, organizations can confidently guarantee recovery when it matters most.

Importance of Immutable Backups: Follow the 3-2-1 backup rule—keep three copies of data on two different media, with one copy off-site—to ensure data availability and integrity. Reliable access to backups is essential for recovery, and the 3-2-1 rule safeguards your data against loss.

ASK YOUR TEAM THESE QUESTIONS:

Can you consistently follow the 3-2-1 backup rule without creating multiple copies of your backups in different locations?

Can you manage the security, compliance, and governance risks associated with having multiple data copies?

Level 2: Backup Security

While backup immutability is essential, it isn't enough for full cyber resilience. If an attack affects both production and backup servers, recovery can be compromised. The second level of the maturity model emphasizes securing not just backup data, but also the backup infrastructure. This involves applying strong security measures to shield backup systems, ensuring the environment is isolated, monitored, and resilient against threats, just like primary servers.

Safeguarding Access: Use strong root access management and multi-factor authentication (MFA) for backup systems to prevent unauthorized access and reduce the risk of compromise.

ASK YOUR TEAM:

How do you manage root access for your backup servers? How are you currently managing MFA for your backups?

Level 3: Cyber Remediation

After securing your backup infrastructure in Level 2, focus on effective cyber remediation to ensure a clean recovery with minimal data loss. Quick recovery is crucial, so organizations need a tested recovery plan for efficiency. Identify restore points and find the latest clean data versions to minimize loss. Certify that recovered data is clean to prevent reintroducing threats into the environment.

Identifying Clean Data: Use techniques to identify clean data for recovery and minimize data loss. Threats often compromise parts of files during their dwell time, complicating recovery and potentially forcing a revert to older backups, which leads to significant data loss.

ASK YOUR TEAM:

How do you choose the cleanest starting point for a restore while minimizing data loss?

Level 4: Cyber Investigation

After establishing remediation processes, focus on cyber investigation. Investigating data breaches and preventing reinfection are crucial tasks that often involve chaotic analysis across various insights and resources. Security teams must piece together a clear incident timeline to understand what happened and decide the best course of action. Throughout the investigation, ensure regulatory compliance to meet legal requirements.

Monitoring for Threats: Monitor unusual access to detect potential threats early. Access attempts from unfamiliar locations often signal a compromise.

ASK YOUR TEAM:

Do you have methods to quickly detect logins from unusual geographies before they can pose a threat to your backups?

Level 5: Enhance Detection

After strengthening your cyber investigation capabilities, focus on enhancing threat detection, especially through backups. Bad actors often target backups by deleting, encrypting, or changing retention policies to hinder recovery. Detect threats early to reduce dwell time and limit attack damage. Establish strong methods for detecting compromises in both backup and production data to boost overall threat detection and reduce risks.

Detecting Compromises: Organizations must establish methods to detect compromises in backup or production data to enhance overall threat detection. When attacks encrypt primary data, Security Operations Center (SOC) teams often lack crucial information about the threat's scope and timeline.

ASK YOUR TEAM:

Protected data serves as a valuable proxy for primary data.

Do you have methods or processes in place to search for threats and identify Indicators of Compromise (IOCs) across your protected data?

Advancing through these levels enables organizations to significantly boost their cyber readiness, strengthen defenses, and enhance incident response capabilities.

How Druva Empowers Customers to Strengthen Cyber Resilience

Druva's Data Security Cloud provides a robust, cloud-native platform that addresses critical gaps in incident response and recovery workflows. Built on secure AWS infrastructure and using a zero-trust security model, it delivers comprehensive protection to help organizations advance through every level of cyber competency, as demonstrated below.

Level 1
Data Immutability

- ➔ Druva stores immutable backups in air-gapped cloud storage with dual envelope encryption.
- ➔ Druva's Data Lock feature prevents malicious or accidental deletion of recovery points.
- ➔ 3-2-1 rule made easy with Druva: 3 copies, 2 locations, 1 offsite/air-gapped, for reliable recovery.

Level 2
Backup Security

- ➔ Ensure fast recovery and continuity with Druva's Data Security Cloud, a SaaS platform with 24x7 availability.
- ➔ Druva isolates and air gaps all backup infrastructure to enhance security by separating the data plane from the control plane.
- ➔ Using a combination of Account Lock, MFA, and SSO, Druva identifies and prevents backup admin accounts from maliciously modifying or deleting data.

Level 3
Cyber Remediation

- ➔ Easily pick the cleanest starting point for a restore, while also minimizing data loss with Druva's Restore Scan and Rollback Actions.
- ➔ Quickly and automatically build the most recent clean copy of backup data across multiple copies with Curated Recovery.
- ➔ Quarantine backups at the snapshot, device, and VM level quickly and easily within the Druva console with Quarantine and Sandbox Recovery.

Level 4
Cyber Investigation

- ➔ Use Druva's Threat Hunting capability to determine the scope, gestation, and timeline of threats to backups that tools within the SOC are unable to provide.
- ➔ Investigate cyber threats in your backup environment by detecting suspicious admins, identifying anomalies, and speeding up incident analysis and response with Dru Investigate — your AI copilot for data security.
- ➔ Anomaly detection (UDA) identifies and responds to threats by understanding your data and sending automated alerts, protecting critical data.

Level 5
Enhance Detection

- ➔ Managed Data Detection and Response (DDR) provides 24x7 security monitoring of backups, expert analysis, and support from Druva Incident Response for threat monitoring, investigation, response, and cyber recovery.
- ➔ Leverage Druva's SIEM integrations and equip SOC teams with insights into the backup environment's security health for cyber recovery.
- ➔ Gain complete visibility with Druva's Security Command Center — get alerts for potential threats and analyze suspicious activity in real time.

As cyberattacks grow more sophisticated and recovery costs climb, organizations must strengthen cybersecurity strategies and adopt comprehensive measures beyond traditional defenses. Druva's Cyber Resilience Maturity Model guides you through five levels to secure backups, enhance threat detection, close gaps, and strengthen defenses, boosting cyber resilience for faster recovery.

Next Steps

How are you identifying your organization's security gaps? Speak to a Druva expert to schedule a Cyber Resilience TableTop exercise.

See why Druva was recognized as a 2024 Gartner® Peer Insights™ Customers' Choice for Enterprise Backup & Recovery Software Solutions and start a risk-free 30-day self-service free trial. No credit card required.

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com