AN OPEN LETTER TO CISOs: A GUIDE TO CONTINUOUS BUSINESS

Dear CISO,

I hope this message finds you well. I wanted to share some insights on how to strengthen cyber resilience and safeguard data against the persistent threat of ransomware. As you are aware, the ransomware attacks we're facing are becoming increasingly sophisticated, and our backup data is not exempt from these threats. Often, the recovery environment is a blind spot for security teams, making it particularly vulnerable.

A RECENT REPORT FROM ENTERPRISE STRATEGY GROUP (ESG) FOUND THAT:

92%

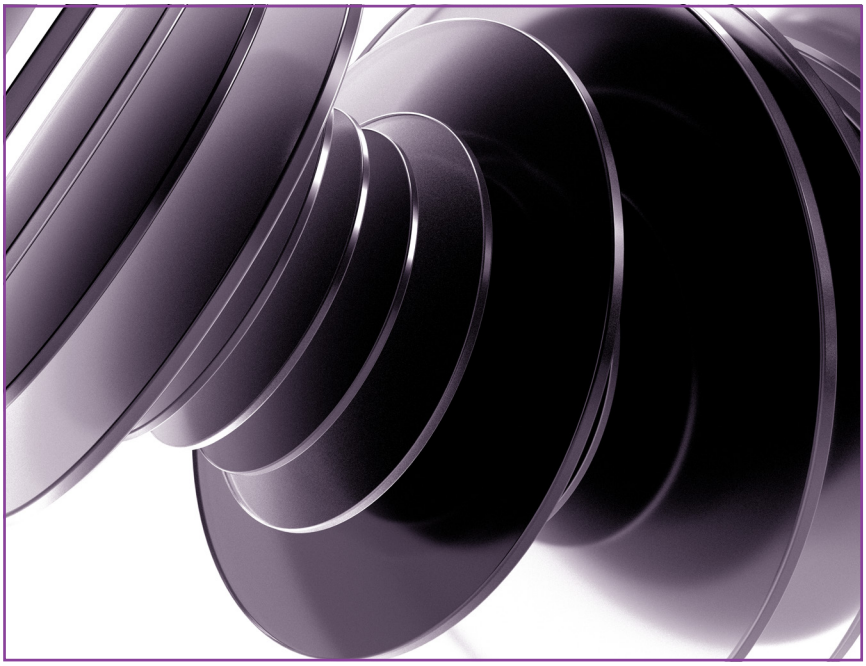
of respondents said they've suffered from attacks explicitly targeting backups.[1]

71%

of respondents said those kinds of attacks accounted for half or more of all attacks.[1]

26%

of respondents are confident in their ability to protect all mission-critical applications and data.[1]



The 2024 Cost of a Breach Report underscores the need for collaboration, finding the average cost of a breach increased 10% to $4.88M and the average time to identify and contain a breach was 258 days.[2]

To address this challenge and mitigate risk, it is imperative that our teams collaborate closely to drive continuous business and recover quickly when the worst happens.

By working together, we can bridge the gaps and enhance our overall security posture.

[1] Preparedness Gap: Why Cyber-recovery Demands a Different Approach from Disaster Recovery, Enterprise Strategy Group, December 2024.

[2] Cost of a Data Breach Report 2024, IBM and Ponemon Institute.

COLLABORATION IS KEY

To make the most of our strategy for continuous business, we need to work closely together. **Here's how we can collaborate:**

01 Establish clear communication channels.

Regular meetings: Schedule regular meetings between IT and security teams to discuss ongoing projects, potential threats, and any issues that need to be addressed.

02 Define roles and responsibilities.

Role clarity: Clearly define the roles and responsibilities of each team member to avoid overlap and maintain accountability.

Joint responsibilities: Identify areas where IT and security teams need to work together and assign joint responsibilities.

03 Develop a unified incident response plan.

Comprehensive plan: Create a comprehensive incident response plan that includes both IT and security teams. This plan should outline the steps to be taken in the event of a cyberattack.

Regular drills: Conduct regular drills to confirm that both teams are familiar with the incident response plan and can execute it effectively. This is critical to getting back to a minimum viable business after an attack.

04 Implement continuous training and education.

Cross-training: Provide cross-training opportunities for IT and security team members to understand each other's roles and responsibilities better.

Ongoing education: Keep IT and security teams updated on the latest cyber threats and best practices through ongoing education and training programs.

05 Utilize shared metrics and reporting.

Common metrics: Establish common metrics to measure the effectiveness of our cyber resilience efforts. This could include metrics like recovery time objectives (RTO), recovery point objectives (RPO), and the number of incidents detected and resolved.

Regular reporting: Implement regular reporting to track progress and identify areas for improvement.

06 Foster a collaborative culture.

Team building: Organize team-building activities to foster a collaborative culture and build trust between IT and security teams.

Open dialogue: Encourage open dialogue and feedback so that both teams feel heard and valued.

EFFECTIVENESS OF CYBER RESILIENCE SOLUTIONS

One tool that we have in-house that can help is Commvault Cloud. You probably think of it as "just a backup tool," but it can help us build cyber resilience.

Commvault Cloud offers a comprehensive suite of security and recovery features that address today's cyber resilience challenges. It provides integrated backup, disaster recovery, and cost-efficient strategies across various cloud environments, including AWS, Azure, and Google Cloud. This helps protect our data and make it recoverable, no matter where it resides.

Commvault Cloud Cleanroom Recovery provides a secure, isolated environment for data recovery. It allows us to identify and remove malware from our recovery environment, enabling a clean and rapid recovery. Key features include air-gapped storage, immutable backups, built-in automation, and AI-enhanced recovery scaling. This solution helps us maintain continuous business, even in the face of sophisticated cyber threats.

Commvault Cloud Rewind goes beyond traditional backup and disaster recovery. It allows us to rewind and rebuild dynamic and distributed cloud applications quickly from outages and ransomware attacks. With features like instant recovery, continuous cyber resilience, and a patented dual-vault cloud time machine, Cloud Rewind keeps our applications available and secure at all times.

WHY COMMVAULT FOR CYBER RESILIENCE?

01

Cyber resilience:

Organizations demonstrating strong cyber resilience are increasingly distinct from those struggling with cybersecurity challenges.[3] This indicates that investing in cyber resilience can provide a competitive advantage.

02

Backup success rate:

Commvault's comprehensive data protection platform helps improve backup success rates by automating processes, providing real-time monitoring, and eliminating the common points of failure found in fragmented legacy solutions.

03

Immutable backups:

Implementing immutable backups, a key feature of Commvault Cloud Cleanroom Recovery, can prevent ransomware from encrypting or deleting backup data, providing an additional layer of protection.

By working together to implement these strategies and with Commvault's advanced solutions, I believe we can create a robust data security and recovery framework that protects our organization from ransomware and other cyber threats, while keeping us on the path to continuous business.

I look forward to your thoughts and collaboration on this matter.

If you want to learn more about Commvault, please check out their website at www.commvault.com.

Best regards,
Your CIO

[3]Global Cybersecurity Outlook 2024 - World Economic Forum