White paper

Best Practices to Reduce Your Cybersecurity Insurance Premiums

Introduction

Today, cyber attacks are becoming more frequent and severe. To safeguard your business, you may be considering cyber insurance, which protects your business in the event of a ransomware attack or other cyber incident.

Before issuing cyber insurance policies, insurers typically ask companies a series of detailed questions to assess their preparedness and cyber risk factors. Just as a home insurance vendor will recommend that you make certain repairs on your home before issuing you a policy, your cyber insurance vendor will often recommend steps you should take to reduce your risk. The good news is that by using a solution like the Druva Data Resiliency Cloud you are substantially reducing your risk – and you can save money on your cyber security insurance premiums as a result. This white paper details 12 best practices to follow so that you can reduce your risk and – and the cost of your premiums.

What factors affect your cyber risk insurance premiums?

Insurers will often require detailed information about your current environment, governance and compliance policies and process, the data you store, and how you protect it. In addition, insurers may also require details about the following:

Previous data loss experiences

Cyber insurance vendors may ask a number of questions about previous experiences related to data loss or damages, including whether you've experienced network-related business interruptions, had any claims made against you, or been investigated for privacy-related violations.

Risk controls

Questions about risk controls may include inquiries into whether you use a firewall, software updates and patching processes, access controls, whether you have a disaster recovery plan in place, whether you outsource critical technology services, and more.

Privacy controls

Cyber insurance vendors want to know if you are in compliance with various regulations and security standards (such as PCIDSS, GLBA, HIPAA, and others), whether you have a formal privacy policy, and more.

12 steps you can take to lower your cyber risk insurance premiums

Here's a list of recommended solutions and processes that many insurers suggest you take to reduce your insurance premiums.

1. Choose a designated Cyber Catalyst product or solution

The Cyber Catalyst^{SM} program identifies cyber security solutions that leading cyber insurers consider effective in reducing cyber risk. The program was created by Marsh, a leading global insurance broker and risk advisor, to help organizations make more informed choices about cyber security products and services. Using a product or service with a Cyber Catalyst designation may lead to enhanced terms and conditions, particularly from insurers participating in the program.

Druva has been awarded the Cyber Catalyst designation for Outstanding Product Security and Ability to Combat Ransomware. This prestigious designation signals that leading insurers believe Druva can help reduce cyber risk.

2. Use strong email security

Despite popular belief, email is not a secure form of communication, and every organization should use caution when sending or verifying sensitive information by email.

3. Implement multi-factor authentication

Multi-factor authentication (MFA) immediately increases account security by requiring multiple forms of verification to prove your identity when signing into an application. Start with email, then apply MFA everywhere it's available.

The Druva Data Resiliency Cloud requires MFA for secure access to products and services.

4. Ensure you're creating full data backups and storing them in a separate, secure location

A full data backup can mean the difference between a complete loss and a complete recovery after a ransomware attack. Develop a strategy tailored to the business.

Druva keeps your backup data in the Druva Data Resiliency Cloud – a secure, offsite triple-replicated storage target.

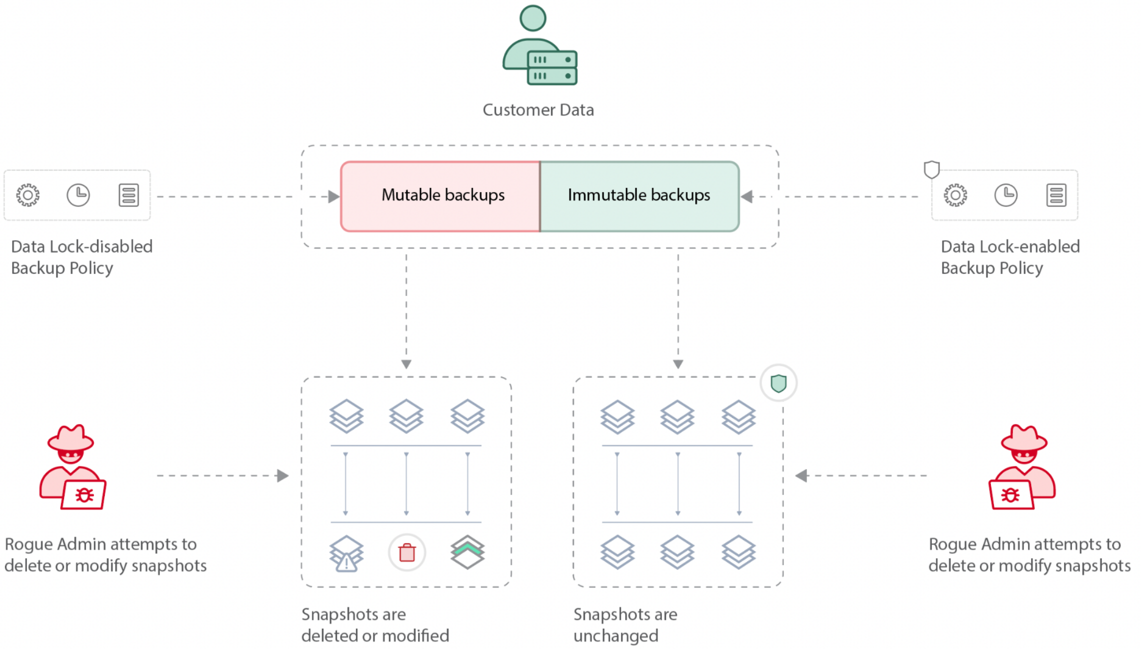
5. Secure remote access

Remote work is more necessary than ever before, which means workers are no longer in controlled work environments. Instead, they are often given access to company resources remotely. When remote access is allowed, the organization takes on additional risks.

6. Use a solution that delivers air-gapped and immutable backups

Truly immutable, air-gapped backups can't be deleted, changed, or corrupted by either an unauthorized or authorized person. Using a no OS-storage and object-based architecture, along with zero-trust security, provides protection against ransomware due to its limited ability to only crawl file system data.

Druva provides air-gapped, immutable backups in object-based storage. This means that ransomware can't execute in Druva's environment. In addition, Druva Data Lock prevents changes (or deletions) to a backup policy and the retention of data once the policy is created. This feature helps customers meet compliance requirements and protects your most sensitive data from deletion by malicious insiders. Druva also offers a self-service Rollback Action feature, which stores deleted backup data in a cache for up to 7 days, allowing self-service recovery or rollback of deleted entities.


Customer Data
Mutable backups
Immutable backups
Data Lock-disabled Backup Policy
Data Lock-enabled Backup Policy
Rogue Admin attempts to delete or modify snapshots
Rogue Admin attempts to delete or modify snapshots
Snapshots are deleted or modified
Snapshots are unchanged

7. Ensure regular patching and software updates

All software presents at least some risk to the organization. Cyber criminals look for vulnerabilities, which can easily be located to prevent exploits through regular software updates. With a SaaS-based data protection solution, patching is taken care of for you.

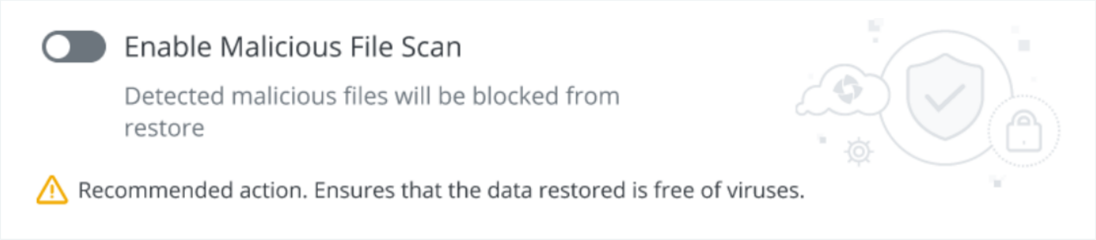
Druva's SaaS-based data protection solution simplifies data security for you. With no hardware or software to manage, you don't need to worry about vulnerabilities, complex configurations, patching, software updates, or monitoring.

8. Use a password manager

Password managers help keep track of multiple passwords and generate new ones at random. They are essentially an encrypted vault for storing passwords that are protected by one master password. These master passwords act as “keys to the kingdom” and should be heavily protected.

9. Scan for malicious software

Endpoint detection and response (EDR) tools (including traditional antivirus and anti-malware software) readily identify, detect, and prevent advanced cyber threats.



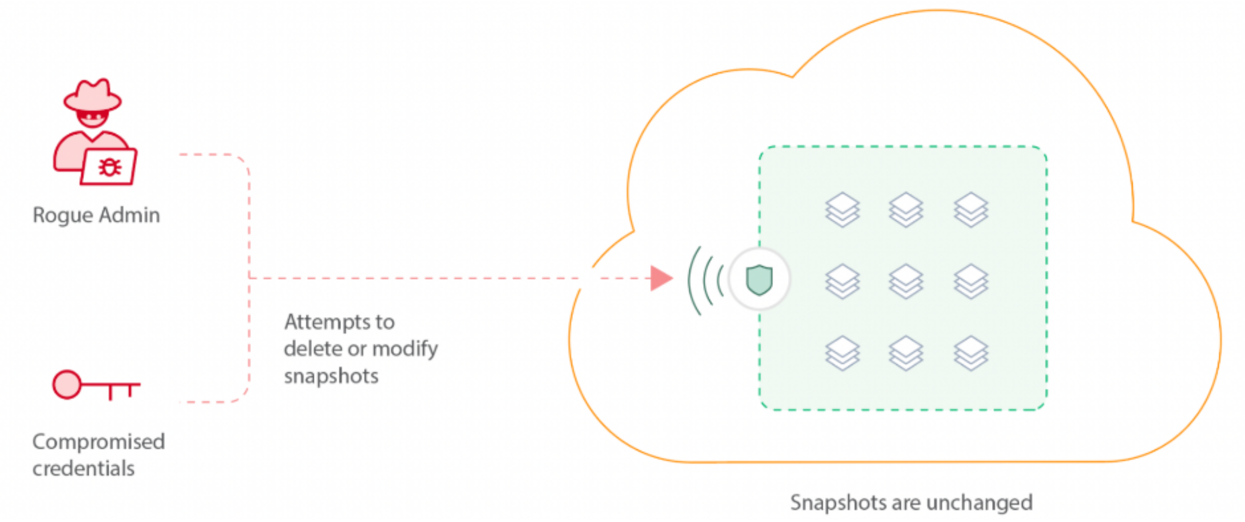
Enable Malicious File Scan

Detected malicious files will be blocked from restore

⚠ Recommended action. Ensures that the data restored is free of viruses.

10. Use data encryption

Encryption is a process that renders data inaccessible to bad actors who manage to steal it unless they possess the key required to access it. If your data is not encrypted and you lose a device such as a laptop, your organization may face a data breach and all of the legal, regulatory, and remediation costs that come with it.



11. Provide security awareness training and oversight by a managed IT help desk

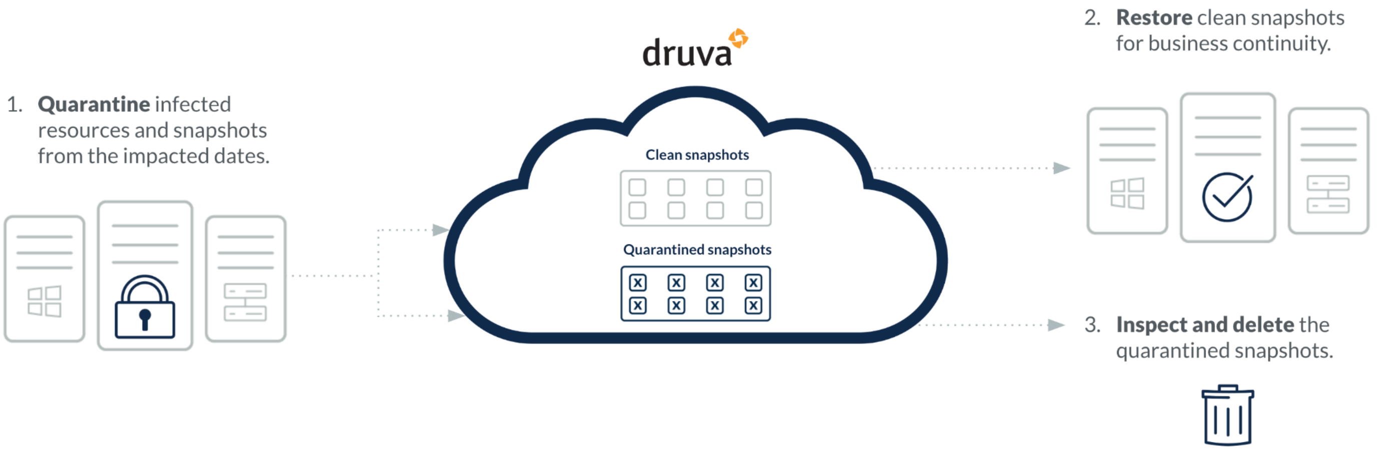
By some estimates, 60% of claims are the result of human error. This can be avoided by creating a culture of cyber risk awareness that holds everyone accountable. Because attacks can occur at any hour, insurers recommend that you have a 24/7/365 help desk that monitors security infrastructure and can take action immediately once an attack is detected.

With Druva’s SaaS-based solution, you can get proactive, human-powered alerts from the Druva CloudOps team to alert you to data anomalies such as unusually large deletions of data.

12. Reduce data loss with automation

If you're hit with a ransomware attack, you want to be able to quickly and easily find the most recent clean version of your files. It can take considerable time and resources to identify clean files to restore.

Druva can add automation to your ransomware incident response by helping your team to quarantine infected resources, support forensics efforts with log data, scan data before recovery, and perform a curated recovery of files to further minimize data loss by automatically finding the most recent clean version of each file across time and adding it to a single "curated snapshot."


druva
1. **Quarantine** infected resources and snapshots from the impacted dates.
Clean snapshots
Quarantined snapshots
2. **Restore** clean snapshots for business continuity.
3. **Inspect and delete** the quarantined snapshots.

Reduce Cyber Insurance Costs and Improve Data Resiliency with Druva

As the only 100% SaaS vendor in the data resiliency space, Druva has a unique advantage when it comes to security posture and data observability. Drua is able to see more data, backup events, and security incidents across more customers and workloads than any other company. Every day, Druva analyzes telemetry from every vertical and size of organization around the world to identify local and global trends. We use those learnings to power security posture and data risk insights as well as develop and deploy product and service improvements for all customers every two weeks via our SaaS delivery model.

The $10 Million Druva Data Resiliency Guarantee

For true peace of mind, Druva offers the Druva Data Resiliency Guarantee. The industry's most comprehensive, this guarantee provides up to $10 million in coverage and guarantees the security, immutability, and availability of your data. The guarantee protects against a wide variety of data loss and downtime events across five key risk categories: cyber, human, application, operation and environmental. The Druva Data Resiliency Guarantee is free for customers who qualify. Learn more.

Next Steps

Contact us to learn more about how you can significantly reduce your cyber security insurance premiums with Druva's 100% SaaS data protection platform.

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
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

Druva is the industry's leading SaaS platform for data resiliency, and the only vendor to ensure data protection across the most common data risks backed by a $10 million guarantee. Druva's innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Resiliency Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.