CYBERARK®

WHITEPAPER

Contain Cyber Insurance Costs and Accelerate Readiness with CyberArk SaaS Identity Security Solutions

Table of Contents

Introduction

The COVID-19 pandemic spurred a surge in ransomware attacks and data breaches across the globe, profoundly impacting the cyber insurance industry. According to data analytics firm Statistica,[1] the number of global ransomware attacks grew from 188 million in 2019 to 304 million in 2020. By the end of 2021, Cybersecurity Ventures estimates global ransomware damage costs will skyrocket to $20 billion,[2] representing 57X more than it was in 2015.

In response, more and more businesses are taking out cyber insurance policies to mitigate risk. A **U.S. GAO report** reveals cyber insurance take-up rates[3] at one major carrier rose from 26% in 2016 to 47% in 2020. Indeed, global insurance company American International Group has seen a 150%[4] increase in frequency for ransom and extortion claim notifications since 2018.

Faced with increasingly frequent and costly reimbursements, cyber insurers are raising premiums and limiting payouts just when businesses need insurance the most. According to an **Insurance Journal** article,[5] cyber premiums in the U.S. and Canada jumped 29% month-over-month in January 2021, 32% in February 2021, and a staggering 39% in March 2021.

Most insurance companies are slashing limits, adding policy exclusions, raising **retentions** and **waiting periods**, and instituting other restrictions. Some providers like AXA have eliminated ransom reimbursement benefits altogether.[6] Most insurers have introduced strict underwriting guidelines, which can drag out application and renewal processes from days to weeks or even months.

Gone are the days when insurers issue policies with few questions asked. Today, underwriters are more discriminating than ever, often denying coverage to high-risk applicants. The days of "one-size-fits-all pricing" and easy discounts are over. These days, underwriters scrutinize each applicant's risk profile and price policies accordingly.

Most underwriters take a close look at a policyholder's security systems and practices to assess risk. They often use open-source scanning tools like **OpenVAS** and **OpenSCAP** to probe customer networks for vulnerabilities and leverage security rating services like **SecurityScorecard** and **BitSight** to evaluate risk. Many partner with outside cybersecurity firms to vet customers.

This whitepaper provides an overview of the criteria underwriters typically use to assess cyber risk, grant coverage and price policies. It provides tips for improving cyber readiness and streamlining the application process. And it explains how the CyberArk Identity Security Platform can help you quickly strengthen your security posture, address underwriter concerns and contain cyber insurance costs.

[1] Statistica website, September 2021

[2] Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031, Cybercrime Magazine, June 2021

[3] Take-up rates refer to the portion of existing policyholders electing cyber insurance coverage.

[4] AIG cyberinsurance ransomware website, September 2021

[5] Cyber Insurance Industry in Crosshairs of Ransomware Criminals, Insurance Journal, July 7,2021

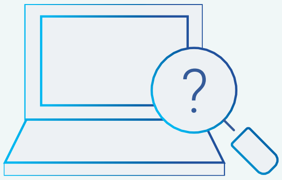
[6] Insurer AXA halts ransomware crime reimbursement in France, AP News, May 6, 2021

Demonstrate Readiness and Check Premium Costs

You can minimize cyber insurance costs by taking a defense-in-depth approach to security and implementing strong security controls and best practices to combat phishing and credential theft and defend against ransomware and data breaches. While every insurer is different, as a general rule, the security systems and practices underwriters typically look for when evaluating risk and pricing out policies include:

- **Multi-factor authentication (MFA) solutions** to positively confirm the identity of remote workers, as well as privileged users like system administrators and third-party IT management vendors. MFA has emerged as a fundamental requirement for cyber insurance—especially in the case of authenticating privileged user access. Many insurers will deny coverage to companies lacking robust MFA controls.
- **Privileged access management (PAM) solutions** to control, secure and audit access to privileged accounts (root, superuser, etc.) used by system administrators and other privileged users. Privileged accounts are typically used for a limited and defined time (I.e., just-in-time) and by approval or workflow.
- **Endpoint detection and response (EDR/XDR) solutions** to proactively identify and remediate suspicious activity on physical and virtual endpoints (i.e., servers and workstations).
- **Privileged endpoint security solutions** to remove local admin rights on workstations and grant users the minimum set of privileges they need to perform their jobs.
- **Incident response plans** to ensure businesses have well-documented detection, containment and remediation procedures in place, including ransomware playbooks.
- **Patch management best practices** to ensure systems are up to date and to minimize security vulnerabilities.
- **Data backup and recovery best practices** to ensure businesses can quickly restore operations in the wake of a cyber attack or disaster.
- **Employee training programs** to improve cybersecurity awareness and educate employees about phishing scams and other tactics used to carry out ransomware attacks.

These days, insurance applicants are often required to fill out detailed questionnaires about their security systems and processes. And they are often asked to back up their responses with evidence.



WHAT TO EXPECT WHEN YOU RENEW YOUR CYBER INSURANCE POLICY

- **Greater security**
- **More questions**
- **Higher premium rates**
- **Lower payouts**
- **Higher retention fees**
- **Longer waiting periods**
- **Drawn-out renewal processes**
- **More frequent renewal rejections**

Strengthen Security and Contain Cyber Insurance Costs with CyberArk

CyberArk offers a comprehensive collection of Identity Security solutions to help you strengthen your security posture, improve protection against ransomware and other threats and keep cyber insurance premiums in check. The CyberArk Identity Security Platform powers a variety of SaaS solutions including:

- **CyberArk Privileged Access Manager** provides foundational controls for protecting, controlling and auditing privileged access across on-premises, cloud and hybrid infrastructure. The solution helps organizations efficiently manage privileged credentials, proactively monitor and control privileged account activity, intelligently identify suspicious activity and quickly respond to threats. Privileged Access Manager supports Adaptive MFA for positively identifying privileged users and controlling access to critical resources. The product is available as both a self-hosted offering, as well as a SaaS solution (Privilege Cloud).

Cyber Catalyst SM

CyberArk Privileged Access Manager has received the coveted Cyber Catalyst SM designation from Marsh, the world's leading insurance broker and risk advisor. The Cyber Catalyst program leverages the aggregated knowledge of leading cyber insurers to evaluate the effectiveness of cybersecurity products in reducing cyber risk. Organizations that adopt Cyber Catalyst-designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers. Privileged Access Manager is the only PAM solution to receive the Cyber Catalyst designation.

- **CyberArk Vendor Privileged Access Manager** provides fast, easy and secure privileged access for all third-party vendors maintaining and supporting corporate IT systems from outside the enterprise network. The solution provides full privileged session isolation monitoring and audit, without the requirements of virtual private networks (VPNs), passwords or agents. In addition, Vendor Privileged Access Manager supports MFA to guard against ransomware and other threats associated with stolen credentials.
- **CyberArk Identity** gives remote users simple and secure access to enterprise applications and services. The solution supports risk-based adaptive MFA functionality across both privileged and non-privileged users to help defend against ransomware and other risks posed by compromised or stolen credentials. Unlike traditional MFA solutions, CyberArk Identity Adaptive MFA uses AI-powered behavioral analytics and contextual information to determine which authentication factors to apply to a particular user in a specific situation, improving end-user satisfaction and productivity.
- **CyberArk® Endpoint Privilege Manager™** reduces security vulnerabilities by removing local admin rights from endpoints and temporarily elevating end-user privileges for specific tasks, on-demand, as required. The solution defends against credential theft by safeguarding passwords and other credentials cached by Windows, web browsers and other programs. Endpoint Privilege Manager also protects against ransomware and other types of malware by intelligently blocking or restricting suspicious or untrusted applications through application controls.

The table below summarizes how CyberArk's solutions can help you address the most common criteria underwriters use to assess risk and price policies.

Underwriter Criteria	CyberArk Solution
Applicant uses MFA to positively identify remote employees	Identity
Applicant secures and controls privileged accounts and uses MFA to positively identify privileged users	Privileged Access Manager
Applicant uses MFA to positively identify remote vendors	Vendor Privileged Access Manager
Applicant removes local admin rights on endpoints and blocks untrusted applications to reduce vulnerabilities	Endpoint Privilege Manager

Accelerate Readiness with SaaS Solutions and Jump Start Packages

When you renew your cyber insurance policy, you may be required to demonstrate cyber readiness on short notice or risk huge premium spikes or outright coverage denial. CyberArk Identity, Privileged Access Manager, Vendor Privileged Access Manager and Endpoint Privileged Manager solutions are all available as cloud-based services for rapid deployment and easy operation. CyberArk SaaS solutions can help you strengthen your security posture and address underwriter concerns and help you show evidence of the pre-audit requirements within a short amount of time.

Whether you are renewing coverage or applying for cyber insurance for the first time, CyberArk's Blueprint for Identity Security Success can help you accelerate readiness. The Blueprint outlines practical steps you can take to address your most pressing security requirements as quickly as possible.

CyberArk also offers Jump Start packages to help you streamline the implementation and adoption of CyberArk solutions and accelerate risk reduction and time to value. Experienced CyberArk Security Services professionals provide expert advice to help you effectively plan, roll out and scale your Identity Security program.

TIPS FOR IMPROVING CYBER READINESS

Take advantage of cyber security education and readiness programs offered by insurance carriers. Many carriers offer policyholders free or discounted risk assessment services, employee training programs, planning exercises and other cyber loss mitigation services.

Use security rating services like SecurityScorecard and BitSight to determine your risk score. These tools often report false positives. Be proactive and resolve issues with rating service providers before underwriters discover them.

Use open-source vulnerability scanners like OpenVAS and OpenSCAP to identify and correct security gaps before renewing or applying for cyber insurance.

CONCLUSION

Ransomware attacks and data breaches are skyrocketing, impacting the bottom line of cyber insurance providers across the globe. Over the past year, carriers have hiked rates and slashed benefits to try to restore profitability. Insurers are far pickier when writing policies today. Nowadays, underwriters assess each applicant's individual risk profile and price policies accordingly.

CyberArk offers a comprehensive SaaS Identity Security solution that meets the core criteria underwriters typically use to evaluate risk and set premium rates. As the leader in Identity Security, CyberArk helps secure privileged access to Tier 0 systems throughout the IT estate, provides risk-based Adaptive MFA for all users and delivers robust protection across all endpoints. The portfolio reduces time to benefit, lowers cost, operates efficiently for the IT team and provides all the standard benefits associated with a modern SaaS solution.

Based on thousands of successful deployments throughout the Fortune 500, only CyberArk has the knowledge and resources to onboard all products and services quickly, easily and in a programmatic way that provides scalable risk reduction.

Next Steps

Learn how CyberArk contains your cyber insurance costs and protects your business.

REQUEST A FREE DEMO

LEARN MORE

- CyberArk Privilege Cloud Jump Start Solution Brief
- CyberArk Identity Jump Start Solution Brief
- CyberArk Endpoint Privilege Manager Jump Start Solution Brief
- CyberArk Privilege Cloud® Datasheet
- CyberArk Vendor Privileged Access Manager Datasheet
- CyberArk Workforce Identity Solution Brief
- CyberArk Endpoint Privilege Manager Solution Brief

About CyberArk
CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice. U.S., 09.21 Doc. WRQ-42

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.