WHITEPAPER

PAM and Cyber Insurance

How Privileged Access Management can lower the price of cyber insurance coverage.

senhasegura

As the demand for cyber insurance increases, so does the pricing and red tape. Discover how these challenges can be overcome with a Privileged Access Management (PAM) solution.

The average cost of a data breach reached an unprecedented high of $4.45 million in 2023*

*According to the IBM Cost of a Data Breach Report.

Introduction

Cyber attacks have surged worldwide, with hundreds of billions occurring annually, driving up the need for enhanced cybersecurity and protection measures. According to the IBM Cost of a Data Breach Report, the average cost of a data breach reached an unprecedented high of $4.45 million in 2023, marking a 15.3% increase since 2020. Companies are grappling with universal rising costs.

In response to these threats, many organizations are not only investing in attack protection but also considering cyber insurance to safeguard business continuity in case of incidents. However, policy costs are rising, and insurers are asking for more proof that strong cybersecurity strategies are in place before agreeing to provide coverage. Many companies may have no choice but to meet such terms, as more organizations are requiring that their business partners have cyber coverage.

In this whitepaper, we will briefly discuss the importance of cyber insurance and its relevance in today's business landscape. We will also explore how the implementation of a Privileged Access Management solution can effectively reduce associated costs while enhancing your company's protection against prevalent modern threats. We hope you find this information valuable.

Happy reading!

Why Cyber Insurance?

Cyber insurance serves as a vital layer of protection within a company's cybersecurity toolkit. Similar to other insurance types, it adheres to well-defined regulations and offers supplementary services, including incident assistance and guidance on implementing best practices. The scope of coverage depends on the insurer and the specifics of the contract. In the unfortunate event of a cyber incident, the insurance should cover either all or a portion of the expenses for data recovery and damage mitigation, and may even include provisions for settling fines.

According to the most recent ITRC Data Breach Report, a staggering 1,802 publicly reported data compromises took place in the U.S. in 2022, marking the second-highest in a single year. Alarmingly, many of these attempts proved successful. IBM's Cost of a Data Breach Report for 2023 underscores the severity, revealing that the U.S. has been the global leader in data breach costs for 13 consecutive years, with an average total of $9.48 million this year. For many businesses, the losses have been incalculable.

In response, two parallel movements have emerged: an increased demand for cyber insurance and the establishment of more stringent criteria by insurers. According to the National Association of Insurance Commissioners, direct written premiums in 2022 amounted to $6.5 billion, a 61% increase from the previous year. Claims have soared by 100%, with payouts doubling over the last three years. Consequently, many insurers have significantly elevated their requirements, with forms extending to 40 pages and rigorous evaluation processes.

This landscape isn't exclusive to the U.S.; it's a global phenomenon. In addition to scrutinizing a company's security architecture, insurers factor in the industry and geographic location of the enterprise, and costs can reach exorbitant levels. While larger corporations may not find this as significant, smaller and medium-sized companies could face insurmountable challenges due to high premiums.

There are avenues to mitigate cyber insurance expenses by implementing fundamental solutions and adhering to regulatory requirements. This proactive approach ensures that a company is not only better equipped to fend off mounting cyber threats but also financially prepared to navigate potential incidents.

Why does cyber insurance cost what it costs?

To explore strategies for reducing insurance rates, it's essential to understand the key factors influencing your premiums:

- Number of Successful Cyber Attacks
- Number of Devices Connected to the Network
- Amount of Data Available or Circulating Recovery Costs
- Security Controls and Best Practices

Let's explore each item.

Number of Successful Cyber Attacks

This factor, while often beyond your organization's control, significantly impacts insurance pricing. It reflects attackers' capabilities and overall security vulnerabilities. If insurers are paying out substantial claims due to successful attacks, they may raise premiums to maintain financial stability.

Number of Devices Connected to the Network

A larger attack surface can be more challenging to manage. Even seemingly simple devices can be exploited by malicious actors. Demonstrating effective device mapping and access control can help mitigate the impact of device quantity on insurance costs.

Amount of Data Available or Circulating

Similar to the previous point, increased data volume requires more stringent controls. Some U.S. states have minimum data security requirements. Implementing sophisticated data management practices can showcase your organization's readiness for incident containment, potentially lowering insurance costs, especially if additional coverage is sought to address fines.

Recovery Costs

The escalating losses resulting from data breaches and incidents prompt insurers to adjust their rates to ensure adequate coverage. IBM reports that the average cost of a data breach in the U.S. is currently $9.48 million. Insurers adjust rates to accommodate these rising costs.

Security Controls and Best Practices

Cyber insurance serves as an additional layer of protection but is not a comprehensive solution. Insurers and prospective policyholders should recognize this fact.

Marcus Scharra, Co-CEO of senhasegura®, offers the following recorecommendations:

- Implement best practices such as Zero Trust and the Least Privilege Principle.
- Establish cybersecurity awareness training programs.
- Identify suppliers and partners (third parties) requiring insurance coverage.
- Implement Multi-Factor Authentication and Privileged Access Management.

Adhering to these practices and investing in robust security architecture and technology tools can help organizations reduce costs and, consequently, lower the risk of falling victim to cyber incidents.

How can PAM help?

"PAM" stands for "Privileged Access Management," a term denoting technologies designed to safeguard, oversee, and control high-privilege accounts, particularly administrative accounts with the authority to make extensive alterations within company systems.

These accounts exist within every organization and are prime targets for cybercriminals. According to Verizon's 2021 Data Breach Investigations Report, a staggering 49% of data breaches involve stolen credentials.

However, those well-versed in this domain recognize that protecting these credentials is no straightforward task. Considerations include:

- Use of strong passwords
- Secure storage of credentials and passwords
- Using Multi-Factor Authentication (MFA)
- Establishment of Access Policy
- And the hardest: convincing individuals of the importance of protecting access and reducing their “powers” within systems.

This list pertains solely to Human-to-Machine (H2M) communications. As we delve into Machine-to-Machine (M2M) interactions, the complexity increases substantially, rendering manual management virtually impossible.

This is where PAM solutions come into play. They comprehensively map all access within an organization's networks and facilitate the enforcement of stringent access policies, creating a secure environment for crucial applications like servers. Moreover, these solutions enable real-time monitoring of all activities during privileged user sessions, enhancing the transparency of IT operations.

As a result, PAM emerges as a fundamental element in bolstering digital security and proves invaluable when considering cyber insurance coverage.

How PAM impacts costs

Incorporating a Privileged Access Management (PAM) solution can significantly expedite the approval of your cyber insurance application. By enabling intricate controls and safeguarding one of the prime targets for cybercriminals—credentials—your company's security stance is bolstered, elevating the likelihood of securing insurance coverage.

A robust PAM solution, when fully utilized, can lead to reduced insurance expenditures through the implementation of the following controls:

Access Auditing

Auditing user and machine activities allows for validation of compliance with best practices and internal policies while enhancing transparency in IT processes. This functionality is particularly advantageous for obtaining certifications and positively influences insurance pricing, demonstrating the presence of auditable security controls within the company.

Third-Party Access Security

The threat posed by suppliers should not be underestimated. Granting access without accountability can result in practical issues and potential surcharges when procuring insurance. A reliable PAM solution establishes a secure environment for third-party access, permitting controlled and monitored access to only the necessary resources.

Session Recording

Session recording functionality acts as a deterrent against privilege misuse and aids in identifying malicious activities, contributing to incident investigations and remediation.

Multilevel Approval Workflows

This feature reinforces security measures and complicates the abuse of privileges within systems. Configurable workflows at various levels ensure comprehensive access review, approval, and activity logging.

Limited Access to Sensitive Information

The volume of data can indeed impact cyber insurance premiums, but not all data holds equal weight. PAM plays a pivotal role in fortifying access controls and safeguarding sensitive information. It encompasses both internal and external measures for data privacy and device protection.

By harnessing the full potential of PAM, your organization can not only enhance security but also drive down insurance costs by showcasing robust security controls and risk mitigation strategies to insurers.

Conclusion

Now that you have an understanding of the key factors influencing cyber insurance pricing and how PAM contributes to cost reduction, it's time to translate this knowledge into action.

To make informed decisions, remember to thoroughly assess your organization's requirements and select the insurance plan that aligns best with your needs. Additionally, consider the controls and solutions necessary for a comprehensive cybersecurity strategy that extends beyond the policy purchase.

If you're uncertain about where to begin this assessment, explore the wealth of resources available from senhasegura to guide you in making informed cybersecurity and insurance choices.

Access Free Materials

Stay safe!

About senhasegura®

senhasegura is a globally recognized Brazilian cybersecurity firm that specializes in cutting-edge technology for Privileged Access Management (PAM). Our expertise extends to assisting companies in combating data hijacking (ransomware) attacks, mitigating insider threats, addressing risky user behaviors, and securing both human-to-machine (H2M) and machine-to-machine (M2M) communications. With our comprehensive and cost-effective platform, we guarantee optimal protection for your organization's critical assets, accompanied by top-tier customer support.