White Paper by Expert Insights

How To Lower Cyber Insurance Premiums And Improve Security With Multi-Factor Authentication

Published
Jan 2023

Expert Insights

Sponsored by
HID

01 Introduction

Organizations today are facing an unprecedented onslaught of cybersecurity threats, which put customer data and organizational reputations at risk. The financial losses incurred by these attacks can be staggering. The average cost of a data breach reached USD 4.35 million in 2022, an existential cost for many SMEs.[1]

There are no easy answers to this problem. Organizations of all sizes need a robust cybersecurity strategy in place to help minimize the risks, utilizing a range of tools and procedures to ensure adequate protection.

However, there is one crucial foundation which all organizations should have in place: multi-factor authentication (MFA). MFA can help organizations to combat cyberattacks by securing access and accounts – and for this reason, it has become a must-have security measure when qualifying for cyber insurance.

In this article, we will cover how organizations can more easily qualify for cyber insurance – while lowering insurance premiums - with the use of a robust MFA solution. But first, let's take a look at what cyber insurance is, what it covers, and how you can qualify.

02 What Is Cyber Insurance, And What Does It Cover?

Cyber insurance, or cyber liability insurance, comprises a number of insurance policies designed to help your organization in the event of a cybersecurity breach. Globally, there are hundreds of cyber insurance providers and policies available, covering a vast range of different scenarios. These policies commonly include:

- The costs of direct expenses from being hit by a network attack. This can include the cost of expert consultancy, forensics, restoring or repairing data, notifying customers of a breach, legal expenses and even PR costs

- Legal costs if a cyberattack causes breach of privacy regulations or contractual agreements, or in the case of a class-action lawsuit

- Costs to profits and legal defense payments in the case of your organization being unable to fulfil contractual obligations due to cyberattacks

- Technology rendered unusable and profits lost due to attacks such as ransomware, and even the cost of ransomware payments to restore access to technology

- Transfer payment fraud caused by social engineering, such as phishing attacks and impersonation scams

- Loss to profits caused by the reputational damage brands often see post-breach – this is often limited to a set period

Not all providers will cover the full range of these policies, however. Many will not cover potential future loss to profits or cover the damages from any loss to your intellectual property - those that do, often have very expensive premiums.

For this reason, cyber insurance cannot replace a robust security framework to stop cybercrime in the first place. Rather, it helps ensure businesses enforce security best practices and offers support if an attack were to take place.

Who Needs Cyber Insurance?

Any organization that stores and manages sensitive information online, uses digital systems, or is highly regulated by state, federal and international agencies, is at risk from cybercrime, and so should consider implementing cyber insurance. If your business relies on technology and processes personal information over the Internet – such as e-commerce, manufacturing, healthcare, critical infrastructure – you should be looking to implement cyber insurance as a high priority.

For small businesses, cyber insurance is critical. SMEs are a prime target for cyber-criminals who know that they are unlikely to have comprehensive (and expensive) security infrastructure in place to prevent network attacks or scams. Should an attack be carried out, SMEs are also more vulnerable – they cannot afford the huge expenses that can come from not having cyber insurance, such as legal costs, ransomware payments, or loss of profits.

How Can You Qualify For Cyber Insurance?

As with any type of insurance, there are certain conditions that must be met to obtain coverage. These conditions can determine if you are eligible for coverage and, crucially, the cost of cyber insurance premiums.

Specific requirements vary by provider, but there are some key requirements that are commonly seen across different security policies. These include:

- Implementing Security Awareness Training, which includes phishing simulation and awareness campaigns

- Ensuring that sensitive and valuable data is regularly backed up to be restored in the case of a ransomware attack

- Regularly auditing and reviewing security procedures and policies

- Ensuring key data is encrypted to secure against data breach and theft

- Ensuring devices are secured against malware, and kept up to date with endpoint security and management

- Compliance with data protection frameworks and procedures such as GDPR

- Implementing identity and access controls with secure provisioning and, crucially, multi-factor authentication

Multi-factor authentication is increasingly becoming a non-optional tool for obtaining insurance. Without it, you could face being denied coverage, or be offered much higher insurance premiums.

03

What Is Multi-Factor Authentication And How Does It Work?

Multi-factor authentication enforces the use of multiple different verification methods when users log-in to their accounts and applications. This helps to prevent account takeover attacks and is proven to be highly effective in stopping identity-related data breaches. MFA is often mandated by many cyber insurance providers – and the most secure MFA solutions can help to keep premiums costs low.

A “factor” is a way of confirming identity when a user requests access to a digital account. The three most common authentication factors are:

- Something you know: a password, or pin

- Something you have: a secure device, such as a smartphone, smart card, or USB key

- Something you are: a biometric check, including a fingerprint or facial recognition

Traditionally, identity authentication has taken place with just one factor: a password. The increasing rise of password-related scams has meant additional security factors are now commonplace, particularly for consumer accounts, but increasingly in the workforce.

For example, when logging into an account with MFA, you may be asked for a password, and then a verification code sent via SMS or an authentication application. Alternatively, you may use a PIN and a fingerprint or facial scan using a trusted smart device.

In the consumer space, MFA is often managed on a per-account basis. For the enterprise, there are a range of MFA solutions on the market that provide centralized authentication controls for all systems and applications. Implementing MFA is an important step, not just when qualifying for cyber insurance but also in establishing a strong cybersecurity posture in the current threat landscape.

04 Why Do Cyber Insurance Providers Want To See MFA?

The explosion of cloud and SaaS applications led to a 307% rise in account-takeover attacks between 2019 and 2021[2], with financial losses caused by account takeover increasing by 90% in 2021 alone. These attacks are often not high–tech or advanced, but instead operate using simple methods, with low costs and high rewards.[3]

For example, attackers may send out phishing emails disguised as legitimate emails to harvest passwords – over 80% of data breaches[4] begin with a compromised password. They can also buy off-the-shelf malware to compromise email addresses and passwords. These attacks are easy to execute at scale, leaving millions of organizations at risk globally.

MFA protects access to sensitive applications, systems, and data by preventing attackers from compromising accounts, even if they have managed to steal usernames and passwords. In fact, research from Microsoft has found that the simple step of mandating MFA can prevent 99.9% of attacks on accounts.[5]

Some insurance providers will not cover breaches caused by internal employee errors.[6] This includes phishing scams where an employee has given an attacker access to an account by accident. MFA helps organizations avoid this scenario by enforcing authentication policies over networks, applications, and devices to prevent unauthorized access, no matter the location.

MFA is therefore an essential security measure to have in place - even if you're not looking for a cyber insurance policy. In May 2021, The Executive Order On Improving the Nation's Cybersecurity[7] signed by President Biden of the US, mandated the use of MFA for all federal agencies, and in Europe, use of MFA is recommended by ENISA guidelines.[8]

05 How To Choose The Right Multi-Factor Authentication Solution

Implementing an MFA solution can help to meet the requirements set by many insurance providers. But not all MFA solutions are created equal, and there are three key areas to consider when looking for a solution to ensure the highest level of protection and further reduce the risk of a data breach - an important way to lower cyber insurance premiums.

Let's take a look at each of these areas in detail:

Phishing-Resistant Multi-Factor Authentication

As we've covered, implementing MFA helps prevent the vast majority of account compromise attacks. But threat actors continue to innovate with new attack methods designed to bypass authentication controls. The most common of these attacks include phishing, push notification spamming, system cookie theft, and SIM swap attacks. For this reason, it is important to look for multi-factor authentication solutions with robust authentication methods and policies designed to withstand these attacks.

In the US, the Cybersecurity and Infrastructure Security Agency (CISA) has released guidance on phishing-resistant authentication. They recommend implementing FIDO2/WebAuthn based authentication, a widely supported authentication method which enables secure, passwordless authentication utilizing trusted devices.[9]

With FIDO, a private key is stored locally on the client device, while the public key is registered with the online service. During a login attempt, the user device proves possession of the private key with a multi-factor authentication check, such as a fingerprint scan. This enables secure, phish-resistant access to accounts, without the use of a password. We therefore recommend looking for a solution which provides FIDO-based authentication.

Support For Various User Preferences And Access Requirements

The best authentication providers offer a broad range of flexible authentication methods to meet your organization's unique needs and support user preferences. There are a range of authentication methods (OTP, PIN, FIDO, biometrics, push notifications, etc.) and form factors (mobile, smart card, security key) available, so it is important to consider the unique needs of your users when selecting a solution.

For example, some users will use biometrics on their personal mobile devices to authenticate, while others may wish to keep private devices separate from work and use a company provided security token instead. Certain industries cannot use smartphones at all: for example, workers in oil rigs, where they are a fire risk, or workers in regions with poor mobile coverage. In these instances, organizations must be able to offer authentication cards or keys to their users.

It is also important to consider that not all methods of authentication are equally secure. Sending an OTP via email or SMS is less secure than biometrics or a push notification – choosing a solution that offers these more secure methods can help to reduce cyber insurance premiums.

Finally, admins must be able to easily manage authentication credentials and devices. In larger organizations, managing credentials for hundreds of users can be incredibly complex and time consuming. We recommend choosing a solution that offers central PKI credential management, and automatically provisions/revokes access when an employee joins or leaves your organization.

Flexible Access Control Policies

Whichever MFA solution you choose should include flexible deployment options to ensure usability and scalability, while meeting the needs and requirements of your organization's own security posture. This includes support for a broad range of authentication methods, but also access control policies which can be configured and fine-tuned.

For example, the question of how many times an authentication attempt is allowed before the system is locked is ultimately dependent on how risk adverse your organization wishes to be. This must be balanced against the needs of users who need to quickly log into their work accounts. Organizations should be able to customize this type of access control policy to ensure consistent security rules are set and maintained thereby preventing unauthorized account access.

Another important access policy is around privileged users. In some organizations, privileged users, such as IT admins with access to sensitive resources and data, must adhere to additional security policies. This may include additional factors of authentication, such as needing to authenticate with both a push notification and a hardware key or biometric check.

They may also need to authenticate more regularly than users with access to less sensitive data. The best authentication solutions will support the configuration and implementation of policies to support this use case.

We therefore recommend looking for a solution that delivers this flexibility – with access control policies that can be deployed across the whole organization at a user- and role-based level. This ensures that MFA security best practices can be met and balanced against the overall needs of the business, managing user convenience and security while enhancing the security of privileged users.

“We therefore recommend looking for a solution that delivers this flexibility – with access control policies that can be deployed across the whole organization at a user- and role-based level.”

06 Finding The Right Authentication Solution With HID

As we've covered, the first step towards meeting requirements for cyber insurance and ensuring premiums are kept low is implementing an effective, secure, and trusted multi-factor authentication solution. MFA is not one-size fits all. With a vast array of solutions to choose from, and numerous use cases and scenarios to account for, it is crucial to choose the right authentication methods and form factors that fit the needs of your organization, either alone or in combination with each other.

Today's organizations must support a wide range of authentication use cases and secure access to both cloud and legacy systems, across different devices, desktops, networks, web and cloud applications - all while meeting evolving security standards and regulations. In addition, there should be minimal to no disruption to their current business workflows and user behavior.

In industries like healthcare, manufacturing, retail, call centers, and law enforcement, multiple users often need to authenticate to the same devices quickly and easily several times a day.

If your organization is in one of these sectors and you are looking to implement secure, flexible authentication with support for biometrics, mobile devices, access badges, smart cards, or security keys, you may want to consider deploying an MFA solution such as HID DigitalPersona.

If you are looking to leverage user mobile devices as simple-to-use, always on-hand authenticators or you are looking to provide your customers with a secure and swift solution to login or verify transactions, you may want to consider HID Approve - an intelligent, scalable, and intuitive solution that enables users to authenticate, access resources or sign a transaction in seconds.

If you are looking to get rid of passwords, FIDO and PKI-enabled HID Crescendo smart cards and security keys provide phishing-resistant authentication by enabling users to securely log in and access networks, workstations, applications, and data, without needing a password. This helps with improving both security and the user convenience, while lowering cyber insurance premiums.

HID's multi-factor authentication solutions are used by organizations of all sizes in various verticals, from banking and financial services, governments, universities, and hospitals, to law enforcement, utilities, and retail - to increase security and enhance the user experience with multi-factor authentication that is easy to deploy, manage, and use.

Moreover, HID also enables IT admins to centrally manage the lifecycle of the digital credentials, from issuance to revocation to ensure access is automatically revoked when an employee leaves.

We recommend HID's MFA portfolio as a robust, future-proof and highly secure suite of multi-factor authentication solutions that ensures compliance and supports a broad range of authentication methods and form factors.

"We recommend HID's MFA portfolio as a robust, future-proof and highly secure suite of multi-factor authentication solutions".

07 Sponsor Of This White Paper

HID is a market-leading provider of identity security solutions for physical and logical (digital) asset authentication. An independent brand of Swedish door and access control provider ASSA ABLOY, HID manufactures and sells a variety of physical and logical access control solutions, as well as secure issuance products to accompany those solutions.

These include smart cards, card readers, card printers and encoders, cloud services, IoT identification technologies, and identity and access management software.

From their headquarters in Texas and worldwide international offices, HID work with organizations in over 100 countries across a number of verticals, including government, education, finance and aviation, helping them to implement trusted physical and virtual environments founded on seamless, secure access.

www.hidglobal.com
Twitter: @HIDGlobal
LinkedIn: @hidglobal
customerservice@hidglobal.com
Tel: 800-872-5359

08 About Expert Insights

About Expert Insights

Expert Insights is a global, independent resource for organizations around the world to research and compare business IT solutions and services. Our number one goal is to help businesses research and find the right solutions to solve their security problems.

References

1. https://www.ibm.com/uk-en/security/data-breach

2. https://resources.sift.com/ebook/q3-2021-digital-trust-safety-index-battling-new-breed-account-takeover/

3. https://www.veriff.com/blog/account-takeover-fraud-statistics

4. https://www.idx.us/knowledge-center/how-compromised-passwords-lead-to-data-breaches

5. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

6. https://www.techtarget.com/searchsecurity/definition/cybersecurity-insurance-cybersecurity-liability-insurance

7. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

8. https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

9. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf