cpl.thalesgroup.com

THALES

Building a future we can all trust

8 Factors to Consider when Buying **Cybersecurity Insurance**

The impact and the cost of cyber-attacks are increasing, especially for small and medium businesses, making the purchase of cyber insurance a necessity for reducing the risk to organizations. This is what you need to know before buying a cybersecurity insurance policy.

1 Identity is at the center of modern cyber-attacks

Credential compromise is the most common attack vector – 61% of data breaches are attributed to stolen credentials. Compromised identities facilitate a wide range of attacks, including ransomware. The average cost of a ransomware breach has increased to $4.62 million, while the total cost of a data breach has increased by 10% during 2020 – 2021. Costs are related to four groups of activities associated with data breaches: detection and escalation, notification, lost business, and post-breach response. Lost business represents the largest share of breach costs (38%)[1].

> The average cost of a ransomware breach has increased to $4.62 million

2 Cybersecurity claims and premiums rise

Small and medium businesses increasingly rely on digital technology to operate. This reliance creates greater cyber risk. If technology and security fail, cyber insurance becomes crucial for ensuring business continuity. Reports indicate that cybersecurity insurance claims have increased during 2021[2]. Increased claims and accelerated losses result in increased premiums - the Council of Insurance Agents & Brokers reported in March 2022 an average premium increase of 34.3% for cyber policies, marking the first time an increase of this magnitude is recorded since the events of 9/11[3]. This increase is projected to continue well into 2022.

3 SMBs are most vulnerable

As cyber criminals mature and advance their tactics, small and medium businesses become the most vulnerable because they lack the capacity – staff, technology, budget - to build strong cyber defenses. SMBs can quickly become easy targets for criminals wishing to attack larger enterprises through complex supply chains. Add the regulatory landscape with extensive security and privacy requirements to understand why cyber insurance coverage is an existential issue for SMBs.

[1] All statistics, IBM 2021 Cost of Data Breach report, available at https://www.ibm.com/security/data-breach

[2] Coalition, 2022 Cyber Claims Report, available at https://info.coalitioninc.com/download-2022-cyber-claims-report.html

[3] Commercial Property/Casualty Market Index, available at https://www.ciab.com/resources/q2-p-c-market-survey-2021/

4 What does a cyber insurance policy cover?

Cyber risk insurance covers the costs of recovering from a security breach, a virus, or a cyber-attack. It also covers legal claims resulting from the breach. Most cyber policies and data breach insurance includes first-party and third-party coverage.

First-Party Coverage	Third-Party Coverage
Damage or loss of data	Network security and privacy liability
Loss of income	Media liability
Cyber extortion / ransomware	Regulatory proceedings
Reputation damage	

When you buy a cyber risk insurance policy, its applicability is global, however jurisdiction for solving disputes is determined in the terms and conditions of the contract. Much like any other type of insurance you can buy, cyber insurance companies offer a variety of policies with varying levels of coverage depending on your organization's risks.

> "Cyber insurance policies have increased on average by 34.3% and will continue to rise in 2022."
>
> Council of Insurance Agents & Brokers

5 Regulatory requirements affecting cybersecurity policies

Even since the enactment of EU GDPR, the regulatory landscape is expanding. The following requirements affect your cybersecurity policies and drive the need for cyber risk insurance.

President Biden's Executive Order on Improving the Nation's Cybersecurity[1]

- "Develop a plan to implement Zero Trust Architecture"
- "Migration to cloud technology shall adopt Zero Trust Architecture"
- "Agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent"

Office of Management and Budget (OMB) Memorandum on Moving the U.S. Government Toward Zero Trust Cybersecurity Principles[2]

- "Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms."
- "For agency staff, contractors, and partners, phishing-resistant MFA is required."

European Insurance and Occupational Pensions Authority (EIOPA) Guidelines on Information and Communication Technology Security and Governance[3]

- "To ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only when strong authentication solutions are used."
- "Undertakings should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with."

ENISA publication Boosting your Organization's Cyber Resilience[4]

- Protect all remotely accessible services with multifactor authentication. Organizations should avoid using SMS and voice calls as authentication methods. Instead, they should consider "deploying phishing resistant tokens such as smart cards and FIDO2 (Fast IDentity Online) security keys."
- All users must use multifactor authentication whenever supported by an application.

UK Government Cyber Security Strategy: 2022 to 2030[5]

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

[2] https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/

[3] https://www.eiopa.europa.eu/document-library/guidelines/guidelines-information-and-communication-technology-security-and_en

[4] https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

[5] https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

6 Best practices for reducing liability and premiums

Insurers don't want to lose money and are doing their due diligence to investigate a company's cybersecurity practices before insuring them. You can reduce premiums if you are implementing good cyber hygiene practices to avoid a breach. Both you and your insurer want the same thing; for you not to experience a cyber incident. Best practices include:

- Implement multifactor authentication
- Raise cybersecurity awareness through regular training
- Effectively manage third-parties and suppliers
- Encrypt your data everywhere
- Keep all your software and firmware updated
- Develop and test your incident response plan
- Undergo regular penetration testing

7 Key factors for selecting the right MFA solution

"MFA is one of the most important cybersecurity practices to reduce the risk of intrusions—according to industry research, users who enable MFA are up to 99 percent less likely to have an account compromised[1]." As such, multifactor authentication is recommended or required by several regulations and is a pre-requisite for obtaining a cyber insurance policy. Even if a business has met all other requirements, they will have a difficult time getting insurance if they haven't deployed MFA.

When selecting the right MFA solution, you should consider a solution that:

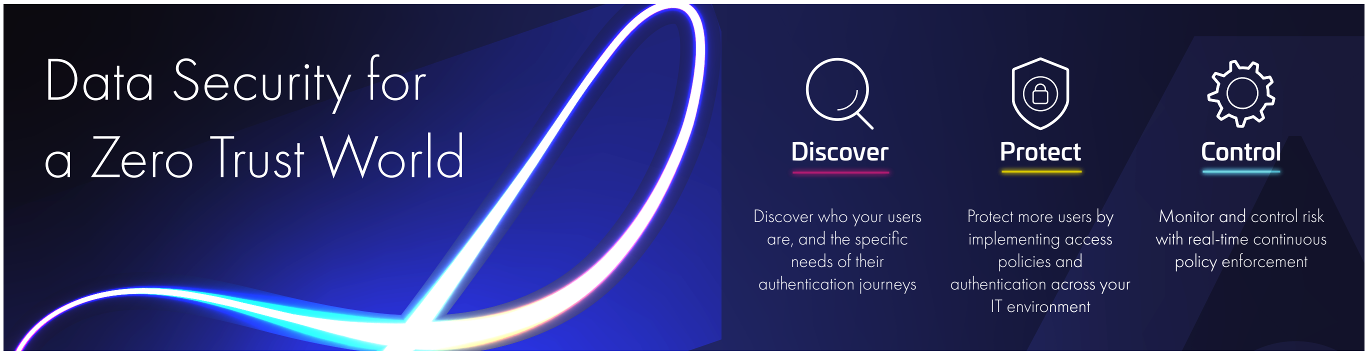
- Offers a choice of authentication methods, including phishing resistant methods such as FIDO and PKI-based MFA.
- Lowers overall implementation and running costs. Getting up and running quickly with MFA will ensure you can get your cyber-insurance policy renewed in time.
- Offers flexibility and scalability by integrating with on-premises and cloud apps.

> "MFA is one of the most important cybersecurity practices to reduce the risk of intrusions—according to industry research, users who enable MFA are up to 99 percent less likely to have an account compromised[1]."

[1] CISA Alert (AA22-074A), https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

8 Ensure cyber insurance coverage with Thales MFA and Access Management Solutions

Thales's SafeNet Trusted Access is an access management and authentication service. It ensures no user is a target by allowing you to expand authentication to all users and apps with diverse authentication capabilities. And it gives you the power to control access to all apps with the right policy that enforces the right authentication method for the right user, in the current circumstances.



Data Security for a Zero Trust World

Discover

Discover who your users are, and the specific needs of their authentication journeys

Protect

Protect more users by implementing access policies and authentication across your IT environment

Control

Monitor and control risk with real-time continuous policy enforcement

With its broad and powerful authentication capabilities, SafeNet Trusted Access meets the specific needs of diverse users by offering the right authentication method for the right user. Offering contextual/adaptive and modern authentication capabilities, through high-assurance FIDO devices, as well as Push and pattern-based authentication, SafeNet Trusted Access allows you to expand secure access to any app and all users, by enabling users to authenticate anywhere, whatever their circumstances.

Integrates with your environment

SafeNet Trusted Access fits into IT environments smoothly and flexibly. Delivered in full SaaS or hybrid mode, it offers the benefits of modern, policy-based access with security by design. Automated workflows and user-initiated enrollment ensure remote support for thousands of users wherever they are, while diverse integration methods ensure you can protect any application – in the cloud, or on-premises.

About Thales's SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

Authentication methods supported by SafeNet Trusted Access

PKI

Hardware

3rd Party

OTP Push

Passwordless

Kerberos

Pattern-Based

Voice

Biometric

Fido

Google Authenticator

SMS

eMAIL

Password