Cybersecurity Insurance for Enterprises

Making an Educated Decision

Digital Security
Progress. Protected.

March 2023

Table of contents

1

What is cybersecurity insurance?

Cybersecurity insurance is still quite a new phenomenon, but has already proven to be a helpful tool for many businesses in recent years. It is designed to protect companies from damages and liability resulting from data breaches and malware attacks. The cybersecurity insurance business is booming against the backdrop of growing concerns about attacks as well as the intensified targeting of enterprises.

Cybersecurity insurance is designed to protect companies from damages and liability resulting from data breaches and malware attacks.

Every organization is vulnerable. Cybersecurity insurance is actually not so much about mitigating risk as it is about anticipating it and transferring its impact. It is a good standard that such insurance is based on **four pillars** that provide enterprises with a complex service consisting of **prevention**, **assistance**, **operations**, and **liability**. A lot of enterprise clients are looking for extra assistance to ensure that they are provided comprehensive care when facing difficult situations. Such demands could be best satisfied holistically, emphasizing a fully tailored and personalized service.

Like any other standard insurance policy, cybersecurity insurance helps businesses reduce the effects of cybercrime, especially those that can have a potentially devastating impact. The digital world throws businesses into various sorts of risks. Then, commensurate threats follow and they keep popping up at breakneck speed.

That requires an ability to fully adapt and react immediately and effectively. Although there is no consistency among insurers about what risks and incidents are covered, enterprises should at least look around for insurance solutions of two types: first-party and third-party coverage. Cyber insurance coverage can and should do more than pay claims; good service is vital in helping you respond to the incident in order to preserve your ability to continue doing business.

> *No insurance will ever prevent an attack from happening – it is just not what it is designed to do. But it is very useful to have cyber insurance after you have had a cyberattack.*
>
> **Rehana Moosa**
> founder of a forensic accounting RMForensics

Key pillars of cyber insurance policy

Prevention

- Pre-breach assessments
- Access to pre-vetted vendors
- Cybersecurity information

Liability

- Legal costs and damages from claims alleging privacy breach or network security failure

Assistance

- Forensic investigators
- Legal services
- Notification
- Credit monitoring
- Call center services
- Crisis management / public relations

Operations

- Costs incurred to keep or return the business to operational
- Loss of revenue, income, turnover
- Costs incurred to restore data and keep the business operational again

Source: Ralf Willems, practice lead of Aon's Cyber Solutions Netherlands, ESET World 2022

2

A growing need for cybersecurity insurance

There have been a lot of recent surveys demonstrating that companies are starting to sing a different song when it comes to a potential purchase of cybersecurity insurance. A 2020 Advisen survey of corporate risk managers showed that 78% had purchased some type of cyber insurance coverage. In 2022, this share increased to 86%. Such a surge of interest in these policies correlates with the fact that attackers are increasingly targeting enterprises. Even though ransomware threats doubled in frequency in 2021 year-over-year, the trend started declining in 2022 and was overshadowed by other types of serious threats.

86%

of corporate risk managers have purchased cyber insurance coverage in 2022

(Zurich's 12th Annual Information Security and Cyber Risk Management Survey, 2022)

According to the latest Allianz's Risk Barometer 2023, cyber incidents are among the biggest company concerns "for the second year in a row", while "cyber insurance claims remain at a high level". This trend is expected to continue in 2023 as many businesses remain vulnerable due to their poor anticipation of the possible risks, eventually resulting in solvency issues or even jeopardizing business continuity.

The types of data that have been compromised the most in the EMEA region in 2022 were credentials and internal data, both with a 67% share, while 79% of actors' motives remained financial. In 2021, 6% of all incidents in the EMEA region were accompanied by data disclosure with a dramatic rise to 30% in 2022. The same report shows that 97% of breaches in this region during the last year were caused by social engineering, system intrusion, and basic web application attacks.

System intrusion, very often caused by a ransomware attack, has persistently increased since 2019 and remains "by far the most common variety" in the Northern America region in 2022. Although not as pronounced, a similar upward trend can also be seen in the EMEA region. However, a disturbing trend in the EMEA, which was observed in 2022, is the rise of social engineering techniques that "illustrates the need for controls to detect this type of attack quickly".

Enterprise businesses are often victims of double extortion tactics, where a hefty payment is demanded to decrypt locked data and to prevent its publication or sale. Criminals may also threaten DDoS attacks on a target's public-facing websites to disrupt business if the ransom is not paid immediately.

30%

of incidents in the EMEA region were accompanied by data disclosure

(Verizon Data Breach Investigations Report 2022)

$1.85

million was the average overall cost of remediating a ransomware attack in 2021

(ENISA Threat Landscape 2021)

90%

of breaches in the North American region were caused by system intrusion, social engineering, and basic web application attacks

(Verizon Data Breach Investigations Report 2022)

The number of ransomware attacks nearly

doubled

in the first half of 2021

(Ransomware attack statistics 2021 – Growth & Analysis, Cognyte)

In 2021, the FBI warned that bad actors were targeting publicly-held companies before major events such as an IPO or merger. The gangs search for non-public information, and then threaten to release any documents that could be financially damaging. The increase in the severity and number of attacks has enterprises worldwide looking to mitigate their risk and potential financial exposure.

Insurance underwriters are looking to mitigate their own risk too, as they face a surge in payouts for a growing number of large claims. One of the trends that we observed approximately two years ago was that insurers were paying out more claims than they were collecting in premiums, while the industry's loss ratio reached 72.8% (2020) after a third-year of constant climbing. The average loss ratio fell to 65.4% in 2021, even as the premiums grew significantly year-on-year. It simply became more expensive for cyber insurers to help companies deal with the cyberattacks.

The present situation is similar and insurers have, therefore, reduced coverage limits, tightened their terms and conditions for coverage, and are imposing more requirements on firms seeking coverage. Increasingly, they are adding exclusions to clarify which cyber events are covered. Some offer ransomware coverage as a costly add-on to another policy or require a separate policy entirely.

> *Be prepared and expect more change.*
>
> **Chris Reese**
> insurance consultant & advisor ESET World 2022

In the United States, the average cost of premiums has increased 25-80% over the last two years, according to insurance provider AdvisorSmith. The average cost of a data breach in the United States in 2022 amounted to $9.44 million, while the costs in the United Kingdom climbed to $5.05 million and to $4.85 million in Germany.

25%

is the approximate average rise of the cost of premiums in the US since 2020

(AdvisorSmith: Cyber Insurance Cost)

12.7%

is the rise of the average cost of a breach worldwide since 2020

(IBM Cost of a Data Breach Report 2022)

Before 2018, data breaches were the biggest cyber threat, so companies holding personally identifiable data, sensitive financial data, and proprietary intellectual property were the most clearly advised to seek cybersecurity insurance. With the rise in ransomware as well as an increase in targeted attacks and advanced persistent threats, enterprises across all industries are targets.

3

How to evaluate policies?

Policies differ widely, so enterprises should work with a knowledgeable broker or agent and examine the fine print closely. Trying to buy insurance with no such assistance might be risky because a broker is the one who can actually help you identify the right coverage that meets your company's expectations and needs. It is quite often the case that companies either don't have enough insurance or they purchased the wrong type of coverage, which is something that can be avoided by professional consultation.

Coverage amounts and sub-limits for ransom payments are important, but how the terms define a covered event is equally important. Make sure it effectively covers ransomware, including coverage for extortion demands and payments, and look closely at how extortion is defined. A small nuance in wording can make the difference between coverage granted and coverage denied.

Two main types of coverage

First-party coverage

This type of coverage is for damages to your business caused by the cyber incident. That applies to situations where your company loses money because of cyberattack.

Examples include:

- costs for legal counsel to determine your notification and regulatory obligations,
- forensic services to investigate the incident,
- recovery of lost or stolen data, recovery of your network and systems,
- customer notification and call center services,
- fines and penalties related to the cyber incident,
- cost of crisis management or public relations,
- lost income due to business interruption

Third-party coverage

This applies to claims filed by others against your company as a consequence of their data loss, or simply due to the fact that they have been compromised.

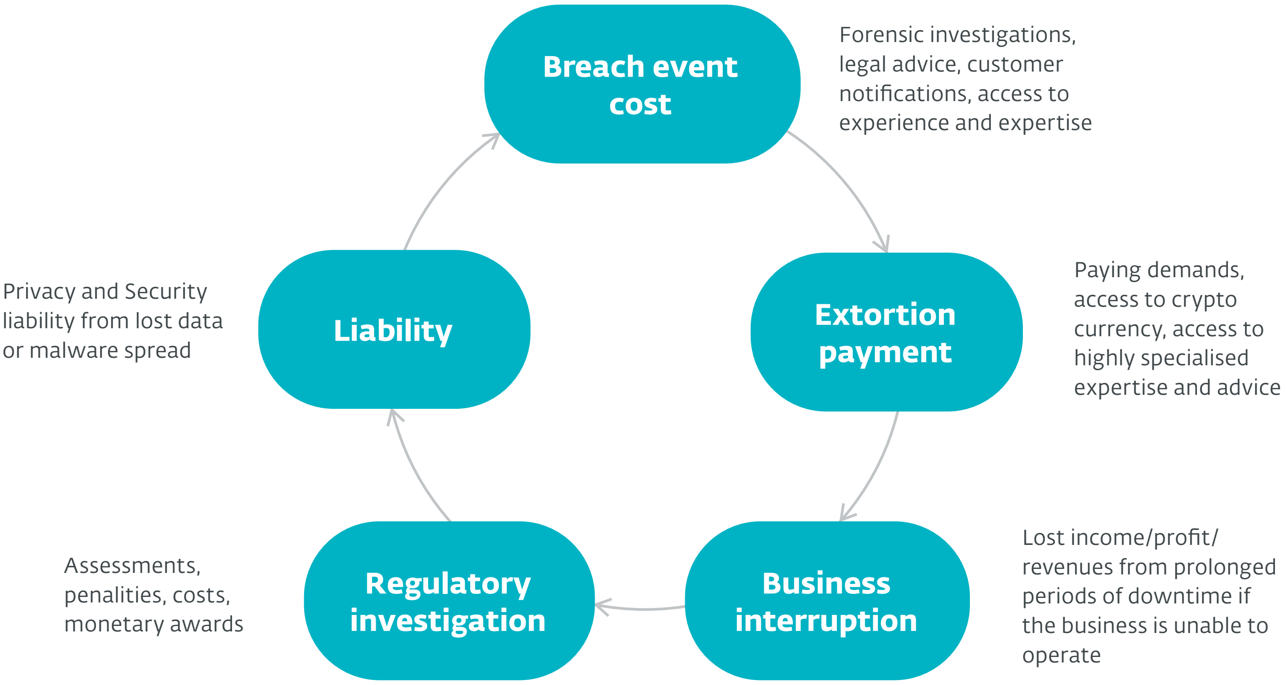
Examples include:

- payments to customers affected by the incident,
- costs for litigation and responding to regulatory inquiries, and
- claims and settlement expenses relating to disputes or lawsuits

Businesses should consider reputational aspects as well. If a company that is in a data business for some time suffers an attack and experiences a data breach, why would their customers want to stay if there is a breach in trust? Customers want to be sure that their data remain safe regardless of the fact that cybercrime happens all of the time. Without this certainty, they could easily start doubting their safety and deem it is too risky for them to stay with such a company. Some of these customers will never come back and it might damage the business' reputation in the eyes of other potential customers.

Event Lifecycle and Coverage Triggers

The diagram below shows how a coverage policy can respond and assist when a ransomware incident occurs


Breach event cost
Forensic investigations, legal advice, customer notifications, access to experience and expertise
Extortion payment
Paying demands, access to crypto currency, access to highly specialised expertise and advice
Business interruption
Lost income/profit/ revenues from prolonged periods of downtime if the business is unable to operate
Regulatory investigation
Assessments, penalities, costs, monetary awards
Liability
Privacy and Security liability from lost data or malware spread

Source: Corinne Cozens, senior underwriter at Axis Capital, ESET World 2022

Good cybersecurity insurance service provision is crucial because it supports your business even when you are not at work. Some ransomware attacks happen after hours and on weekends, so look for a 24-hotline for reporting the incident. Insurers should also have experts who can assist you with legal advice, mount an effective response, negotiate with attackers, and recover your data and systems.

4

Qualifying for coverage

Having cybersecurity insurance to protect you against losses does not mean that you can let your guard down. The opposite is true: Underwriters will not grant coverage unless you have good cybersecurity measures in place.

At a minimum, you can expect to complete a questionnaire, but some insurers will require an assessment by a cybersecurity firm, possibly including penetration testing to probe your defenses. They may also require that you provide regular, in-depth cybersecurity awareness training across your organization. The maturity of your security environment will impact your coverage limits, premiums, and whether or not you can get coverage.

Insurance underwriters all have different ideas about what constitutes effective security, but the requirements are typically some combination of the following:

ENDPOINT SECURITY

Currently, modern endpoint security needs to be multilayered in order to stop today's malware, and it should also be coupled with detection and response capabilities. Extended detection and response (XDR) is a current standard that uses behavioral analytics across endpoint, network, cloud, email protection, and other layers to spot suspicious activity and stop attackers before they can make an impact.

MULTI FACTOR AUTHENTICATION (MFA)

Multifactor authentication as a method for protecting user data from being exposed to unauthorized third parties should be used for all remote access, on privileged accounts as well as for securing backups. MFA can be mobile-based and based on hardware tokens.

CYBERSECURITY TRAININGS

Regular employee cybersecurity awareness training that deepens staff knowledge and allows for managing human-shaped risks, which usually include overlooking both real and potential threats and an inability to react properly when encountering them and, therefore, jeopardizing organizational security.

REGULAR DATA BACKUPS

Performance of regular data backups is like having a safe: It is a precautionary measure taken to store what you value or need the most while being able to restore or access it anytime. Regular backups using encrypted cloud storage that cannot be overwritten by an attacker, even in cases where administrative privileges are gained, is crucial.

REGULAR PATCHING & UPDATES

Regular patching and updates as well as the retirement of systems that are no longer supported is considered as one of the basic precautionary measures that every business should take. It enables you to use fully functional software and tools that prevent you from encountering unexpected incidents that may jeopardize your operational capacities.

PASSWORD POLICY

A strong password policy and secure provisioning process for access rights and permissions – another basic measure that has become notorious over the last two decades due to the fact that many businesses and organizations ignore it at their own peril.

EMAIL FILTERING

Email filtering is an automatic process that rejects, allows passage, quarantines, or modifies incoming messages to protect you against malware and by blocking any possible phishing attacks. Email filtering is best done outside of the endpoint so that you can completely avoid interacting with suspicious emails – minimizing the attack surface. This tool can be very helpful for employees across the organization.

DISASTER RECOVERY

As a strategic measure, plans for disaster recovery allow you to anticipate the possible critical events resulting in system failure or its destruction as well as to handle challenges such as power outages, security incidents, or even natural disasters without any major loss or damage.

TABLETOP EXERCISES (TTX)

A TTX is closely related to disaster recovery as a strategic measure. It is a discussion-based activity that "takes participants through the process of dealing with a simulated disaster scenario". It verifies strategies and emergency practices, and its purpose "is to evaluate an organization's preparedness for a particular disaster and to inform the required participants of their roles in the response".

INCIDENT TRIAGE

Usually done by CISOs and their teams, triaging is crucial for providing answers to questions such as what really needs to be protected. Prioritization, according to the level of importance of a service currently under attack, is closely related to business and compliance requirements. There is a well-known formula supporting prioritization: severity + impact = priority.

CONFIGURATION MAINTENANCE

This includes managing the Active Directory and the proper maintenance of your Office 365 configuration, for example. Active Directory "stores information about objects (e.g., servers, volumes, printers, and the network user and computer accounts) on the network and makes this information easy for administrators and users to find and use." Properly configured Office 365 can prevent your organization from losing files and emails, data exfiltration, or malicious encryption of files. Good configuration maintenance mitigates the risk of forging and stealing your sensitive data.

NETWORK SEGMENTATION

Network segmentation is a security practice and in-depth defense strategy. It enables you to internally divide the network into multiple, smaller subnetworks to better protect sensitive data and limit lateral movement to the rest of the network by controlling the traffic flows via routers, switches, bridges, etc. Network segmentation should address a number of attack techniques, including domain trust discovery, exploitation of remote services, and data manipulation.

PENETRATION TESTING

This measure could be best described as "a cybersecurity technique that organizations use to identify, test, and highlight vulnerabilities in their security posture". It is carried out by ethical hackers (both in-house employees or third parties) who "mimic the strategies and actions of an attacker to evaluate the resilience of an organization's computer systems, network, or web applications."

VULNERABILITY SCANNING

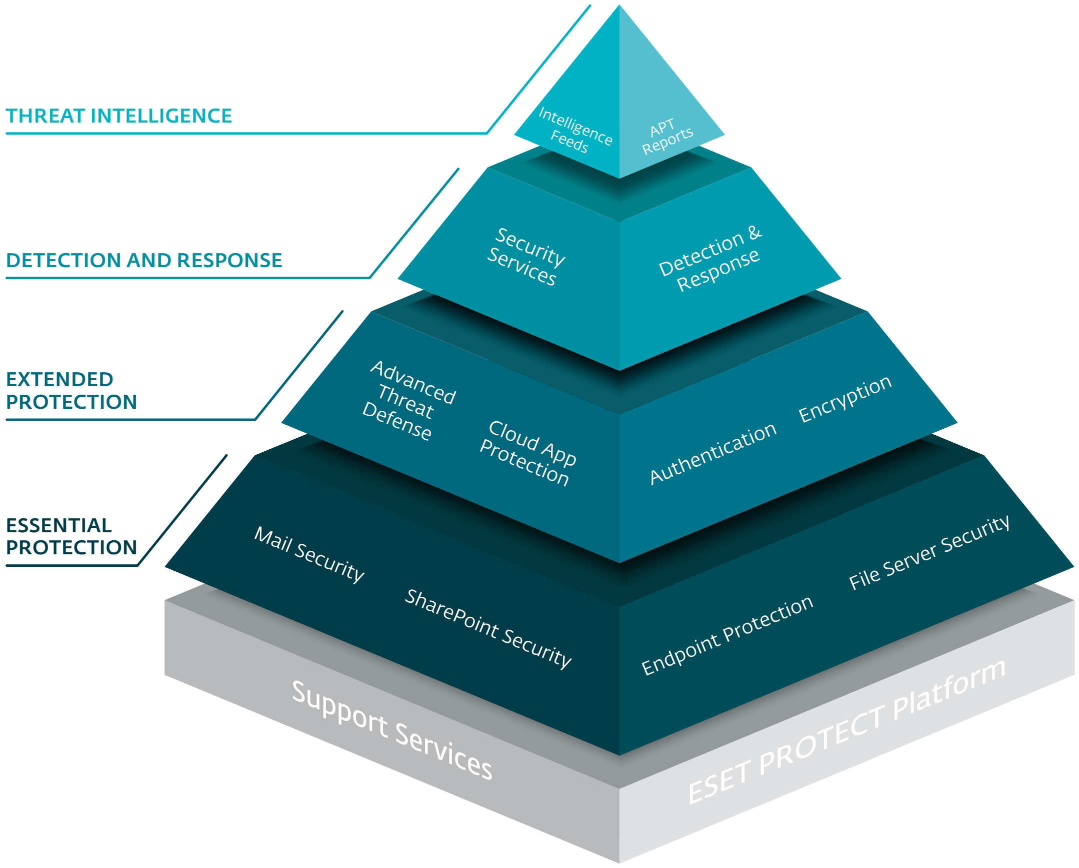
Unlike penetration testing, vulnerability scanning as a stand-alone tool, searches for already known vulnerabilities within the system, and it is performed as a regular automated process taking place across your organization's network. Its main purpose is to prepare input data for up-to-date security reports upon which you manage the process of patching the system. This makes it very closely associated with the practice of conducting regular patching and updating.

Note: This is for informational purposes only and should not be construed as legal advice.

5

Improve your posture with ESET and get better cyber insurance

The ESET PROTECT Platform enables you to significantly strengthen your cyber control. This is crucial for not only lowering your cyber exposure, but also for negotiating better cyber insurance coverage. See how the individual technological protections from ESET help you build a formidable, highly resilient security stack.



THREAT INTELLIGENCE

Not necessarily a requirement from cyber underwriters – but in case you want to get our best research to work for you, this is the best way. In-depth and actionable intelligence from ESET's world-renowned lab, provided via feeds and reports, which will fortify your organization against APTs, botnets, and other types of attacks.

DETECTION AND RESPONSE

Maximum protection, complete cyber risk management, and granular visibility into your IT environment via ESET's most comprehensive detection and response. Access world-leading expertise via ESET MDR and XDR via ESET Inspect. ESET experts help you fine-tune your security posture and provide 24/7 threat monitoring.

EXTENDED PROTECTION

Cloud-based threat defense against targeted attacks and new threat types, especially ransomware, plus dedicated protection for cloud office suites. Improved data and identity with easy-to-use multi-factor authentication and encryption solutions to harden access protection.

ESSENTIAL PROTECTION

Multiple layers of prevention and detection, leveraging ESET's unique technologies, which work together to protect your organization's endpoints, file servers, mail servers, and SharePoint. It includes a hardened browser and specialized controls to deflect RDP compromise. It also includes Mobile Device Management (MDM).

ESET PROTECT Platform and SECURITY SERVICES

Access tailored support appropriate to your needs, plus deployment and configuration assistance. ESET PROTECT, ESET's unified security management platform, delivers XDR and threat-hunting capabilities. It also enables you to implement a zero trust approach for the highest level of cybersecurity.

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide.

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

Digital Security
Progress. Protected.

welivesecurity™