# Protection against digital threats is now a necessity for businesses, not an option

**Monday 14 September, 2026**

**Related Sectors:**

Computing & Telecoms ::

**Scan Me:**

**Warsaw, POLAND - Cyber threats are currently among the fastest-growing business risks faced by Polish enterprises, according to data from CERT Polska and analyses presented in ERGO Hestia's "nieOdporni" ("nonResilient") report. The growing number of security incidents CERT Polska records each year demonstrates that cybersecurity is no longer a concern solely for large corporations, but also for small and medium-sized enterprises.**

**Poland among the countries particularly vulnerable to cyberattacks**

Poland is currently among the countries particularly vulnerable to cyberattacks. In the first half of 2025, it ranked first in the world in terms of the number of ransomware attacks. At the same time, it remains one of the markets with the lowest level of cyber risk insurance coverage. The scale of the threat is also illustrated by recent incidents. One such incident was an attack on software belonging to a company specialising in electronic medical records. The stolen data contained information concerning, for example, prescriptions and the health of as many as 19 million people.

Data from the "nieOdporni" report, Mastercard and other analyses cited by ERGO Hestia show that cyberattacks and data breaches have affected a significant proportion of Polish enterprises.

**Cybersecurity of Polish businesses in figures**

| Indicator | Small businesses | Medium-sized businesses | Large businesses |
|---|---|---|---|
| Experienced a cyberattack | 25% | 44% | 50% |
| Have not provided cybersecurity training | 54% | 14% | 4% |
| Have an incident response plan | 18% | - | 78% |
| Consider the risk of a cyberattack to be high* | 5% | 21% | 18% |

Data are taken from the report entitled “Historia niejednego ataku, czyli cyberbezpiecze?stwo w polskich firmach – wyniki badania Mastercard” (“A Tale of Many Attacks: Cybersecurity in Polish Companies – Mastercard Survey Results”).

*Among businesses that have already experienced a cyberattack, this percentage rises to 25%.

According to the “nieOdporni” report, 88% of Polish organisations have experienced a cyberattack or data breach in recent years. At the same time, an analysis by ScamWatchHQ cited in the report indicates that approximately 69% of businesses in Poland have experienced at least one cybersecurity incident. The difference between these figures results from the different scope and methodology of the studies.

**Awareness of the risk is not always matched by preparedness**

Mastercard’s data reveal a clear gap between the actual scale of the threat and how it is perceived. A total of 71% of small businesses consider the risk of a cyberattack against their organisation to be low, even though one in four has already experienced such an attack.

Across the market as a whole, the problem also concerns basic security measures. The ScamWatchHQ report stresses that only approximately 59% of Polish businesses use basic security software, while more than one-third do not even have basic safeguards in place.

The scale of the risk is further illustrated by data from the BIK 2025 Anti-Fraud Report. Almost 32% of SMEs encountered attempted financial fraud in 2025, while 19.2% fell victim to a hacker attack or faced the risk of internal fraud.

**What cyber threats affect SMEs and what are their consequences?**

The most common threats include ransomware attacks that block access to data and systems, phishing that leads to user accounts being compromised, Business Email Compromise (BEC) fraud, the theft of customer data and intrusions into cloud systems.

The effects of cyberattacks are multidimensional and affect almost every area of a company’s operations. The consequences of cybersecurity breaches in the SME sector are financial, operational, legal and reputational. The most significant include:

- financial losses – the costs of remedying the effects of an attack, recovering data and dealing with business interruption, as well as any ransom payments in the event of ransomware attacks;

- business disruption – the temporary unavailability of IT systems may result in the suspension of production, sales or the provision of

services;

- data loss – the disclosure or destruction of customer and employee data and business information may have long-term consequences for the operation of the business;

- loss of reputation and customer trust – a security breach undermines a company's credibility and may lead to the loss of business partners and reduced competitiveness;

- legal and regulatory consequences – personal data breaches may result in an obligation to report the incident and the imposition of administrative fines under data protection legislation;

- disruption of business relationships – business partners may limit their cooperation with a company that fails to ensure an appropriate level of information security;

- theft of intellectual property – the loss of technical documentation, designs, know-how or trade secrets may weaken a company's competitive advantage;

- increased operating costs – following an incident, businesses often incur additional expenditure on system upgrades, security audits and employee training;

- in extreme cases, a serious cybersecurity breach may threaten the continued operation of the business.

- renewing security software licences;

- maintaining network and server infrastructure;

- security monitoring and incident response services (SOC/MDR);

- regular system updates;

- security audits and penetration testing;

- cybersecurity training for employees;

- the remuneration of IT specialists or fees for outsourced security services.

**How much does a cyberattack cost, and how much does cybersecurity cost?**

The cost of a cyberattack may amount to hundreds of thousands of zlotys and, in the case of serious incidents, exceed PLN 1 million. Analyses by cyber insurance brokers (“Cyber Insurance for Small Businesses in Poland – Key Statistics 2025”, Kelot, 2025) indicate the following average loss levels depending on the size of the business:

| Size of business | Average loss following a cyberattack |
|---|---|
| Small businesses | PLN 50,000–200,000 |
| Medium-sized businesses | PLN 200,000–500,000 |
| Large businesses | More than PLN 1 million |

The scale of investment and the fixed costs associated with maintaining and improving cybersecurity systems in the SME sector depend primarily on the size of the business, its level of digitalisation and applicable regulatory requirements. For most small and medium-sized enterprises, such expenditure represents a significant item in the IT budget.

Cybersecurity expenditure increases with the size of the business, while the annual budget for basic protection is many times lower than the average ransom payment of approximately PLN 200,000–300,000.

The most significant fixed costs include:

Cybersecurity expenditure is generally estimated to account for between 5% and 15% of the total IT budget, and may reach as much as 20–25% in higher-risk sectors such as finance and healthcare.

**How can a business be protected against a cyberattack?**

“Unlike large corporations, small and medium-sized businesses often have neither formal security procedures nor advanced security systems. The absence of specialised IT or security departments makes them an easier target for both conventional criminals and cybercriminals. A cyberattack, break-in or theft may result not only in material losses, but also in business interruption and data loss. Effective protection requires monitoring, access control systems and physical and cyber safeguards to be integrated into a single ecosystem,” says Adam ?liwi?ski, Vice-President of the Management Board of Seris Konsalnet Security, as quoted in the ERGO Hestia report.

According to Tomasz Dolata, a cyber insurance expert at ERGO Hestia, the most effective way to limit the consequences of a cyberattack is to invest simultaneously in comprehensive insurance cover and the development of increasingly robust IT infrastructure. “This makes it possible both to reduce the likelihood of incidents occurring and to minimise their financial and operational consequences,” he emphasises.

The experts quoted in the ERGO Hestia report stress that cyber insurance does not replace technical safeguards such as multi-factor authentication (MFA), backups or employee training. It does, however, provide an additional layer of protection that helps a business limit the consequences of an incident when an attack succeeds despite the safeguards in place.

**What should cyber insurance cover?**

1. attacks, including ransomware, phishing, user account compromise and data security breaches;
2. data recovery and system restoration, as well as digital forensics costs;
3. losses resulting from business interruption;
4. liability towards customers and business partners, including the settlement of claims brought by customers or partners as a result of a data breach or service disruption;
5. legal costs;
6. costs associated with breaches of data protection legislation;
7. crisis management, including crisis communications, communication with customers, helpline services and measures to limit reputational damage;
8. 24-hour access to incident response specialists.
9. the scope of cover and the list of risks covered, for example whether it protects data stored in the cloud and covers remote working and mobile devices;
10. exclusions from cover, for example whether cover also applies when an incident results from an employee error;

11. the insured amounts and liability limits for individual types of loss;

12. the possibility of extending the cover as the business develops;

13. the availability of assistance services;

14. the procedure and time required for claims settlement;

15. the amount of the policyholder's contribution to a claim (the excess).

In addition to comprehensive insurance cover, the policy also covers the services of digital forensics specialists. This is an extremely important component of cyber insurance because, following an incident, a business must not only limit its consequences, but also quickly determine the source of the attack and preserve evidence.

**What should be considered when choosing cyber risk insurance?**

**What should insurance for small and medium-sized enterprises include?**

An optimal insurance package should primarily include protection for company property (buildings, furnishings, machinery and electronic equipment), third-party liability insurance, business interruption insurance, electronic equipment cover, business assistance, legal protection and comprehensive cyber insurance covering both the financial consequences of an incident and specialist expert support.

**Cyber insurance as an additional layer of protection**

As the authors of the "nieOdporni" report point out, a cyber insurance policy provides a financial buffer that enables a business to survive the consequences of a successful attack by covering a ransom payment, funding expert assistance, restoring systems and covering potential fines.

"Protection against cyberattacks is not a choice between 'investing in technology' and 'buying insurance'. Both are necessary. Technology and procedures reduce the likelihood of an attack occurring in the first place. Insurance protects the business if, despite its best efforts, an attack nevertheless occurs," the ERGO Hestia experts state.

Cyber insurance is also readily available today, including to smaller market participants. According to the report prepared for ERGO Hestia, cyber insurance is offered by a growing number of major insurers operating on the Polish market, and the available products also cover small and medium-sized enterprises. The requirements imposed on businesses seeking cyber insurance are achievable: basic safeguards such as a firewall, multi-factor authentication (MFA), regular backups and

the use of up-to-date software supported by its manufacturer are generally sufficient.

Cyber insurance does not have to be expensive. According to the ERGO Hestia report, the average cost of cyber insurance is approximately 0.14% of a company’s annual turnover, representing only approximately 1.8% of the costs that a business may incur following a successful cyberattack. In practice, this means that the cost of the policy is usually incomparably lower than the expenses associated with business interruption, data loss, crisis management or liability towards customers.

Source of information: PAP MediaRoom

**Contact information:**

Marcin ?ebrowski

media@ergohestia.pl

+48 727 024 270

## Company Contact:

_

**news aktuell**

E. desk@newsaktuell.de
W. https://www.newsaktuell.de/

View Online

**Newsroom:** Visit our Newsroom for all the latest stories:
**https://www.newsaktuell.pressat.co.uk**