bilingual edition

ptsoc {news}

17

Cyber Risks insurance:
When reality sharpens ingenuity

3 questions to Pedro Figueiredo,
Zurich Portugal

Managing Cybersecurity Risks in Organisations

.pt

Cyber Risks insurance: When reality sharpens ingenuity

Covering so-called Cyber Risks is relatively new in the insurance industry. It all started on a beach in Hawaii in April 1997, during the International Risk Insurance Management Society annual convention. Originally, the idea was mainly focused on offering a product capable of protecting companies whose data had been stolen from their servers.

Almost three decades later, the world of IT in 2025 is quite different - and, above all, much more dangerous. According to recent projections, the Cyber Risk insurance market should reach $16.3 billion by 2025 and rise to almost double that ($30 billion) by 2030.

This insurance market data closely follows the increase in attacks and losses related to cybercrimes, which have soared to $9.5 trillion by 2024, a significant increase on the $600 billion recorded in 2018.

Eurostat numbers for 2022 show that, in Portugal, only 10 % of companies have Cyber Risks insurance, which is half the European average and a long way off the leading country, Denmark, where 56 % of companies have taken out this type of coverage.

Ransomware and Malware as a Service

One of the fastest-growing types of cyberattack is ransomware, which consists of encrypting a company or organisation's data to prevent normal access, followed by a ransom demand in exchange for the cryptographic key to make the data readable again - hence its name. The first known ransomware dates back to 1989 (before the first Cyber Risks insurance), but this type of cyberattack has only become more common since 2016.

According to the latest report from the Portuguese National Cybersecurity Centre, phishing is still the most common cyberthreat in Portugal. As this is a social engineering technique that often takes advantage of the distraction, lack of knowledge and/or lack of training of employees of companies and institutions, it is also one of the ways most used by cybercriminals to inject ransomware into equipment, networks and systems.

The global cybersecurity landscape is now facing yet another challenge: the use of AI tools to increase the sophistication and ease of attacks. According to the World Economic Forum, 'the rise [of AI-based attacks] (...) is changing the cybersecurity landscape.'

In addition to the sophistication of attacks - such as deepfakes - AI tools also encourage the use of 'Malware as a Service' by new stakeholders with less technical sophistication who would otherwise chose other types of criminal activity. A recent

Europol study even considers cyberattacks to be 'the apogee of "Crime as a Service".'

SMEs and Compliance

In issue 15 of PTSOCnews, in which we analysed NIS2 in greater depth, we had already identified many of the obligations that essential and important entities are subject to in terms of adopting strict security measures and, subsequently, timely reporting them to the competent authorities.

What is challenging, however, is that micro, small and medium-sized companies account for 99.9% of non-financial companies in Portugal - and that these companies, according to a recent report by consultancy Marsh, have cybersecurity controls that are, on average, 15 % lower than those of large organisations, highlighting, for example, the lower implementation of multi-factor authentication strategies. Furthermore, according to the same study, only 40 % of SMEs test their incident response plans, compared to 61 % of large organisations.

These shortcomings on the part of companies are all the more serious given that the NIS2 directive assigns the management of organisations direct responsibility for cybersecurity, namely by requiring supervision, training and allocation of adequate resources for the implementation of security practices.

In this context, it is important to remember that the effective management of cybersecurity risks in organisations requires the adoption of structured methodologies to systematically identify, assess and mitigate threats.

The Portuguese National Cybersecurity Centre (CNCS) has a Guide to Information Security and Cybersecurity Risk Management. In it, it proposes an approach based on international standards such as ISO 31000 and ISO/IEC 31010.

Also at European level, the European Union Agency for Cybersecurity (ENISA) published the Compendium of Risk Management Frameworks with Potential Interoperability; the document analyses various risk management frameworks, including those mentioned above, and highlights the importance of interoperability between them.

Cyber Risks insurance

Cyber Risks insurance, despite being risk coverage products, can play an important role in helping companies to be better prepared in terms of cybersecurity - in addition to the risk coverage itself.

This happens because, as João Lopes from Guardian Seguros told PTSOCNews, 'in most cases, when these insurances are taken out, companies accredited for this purpose carry out an analysis which identifies

Foto: ImageFlow, adobe stock

the company's reality, points of weakness and proposals for improvement - information that the vast majority of entrepreneurs in Portugal do not have when it comes to their company.'

Moreover, these insurances almost always include civil liability components - crucial for any company that holds data on customers and suppliers that could be compromised in some way - as well as capital for legal support and possible ransomware situations.

'The most important thing,' says João Lopes, 'is that the company can quickly return back to its normal operations,' since situations such as a ransomware attack or claims for compensation for data loss often involve significant sums of money and, in the case of organisations with smaller resources, may even force the company to close.

Unlike other more common types of coverages, calculating Cyber Risks insurance premiums is not straightforward. Also according to João Lopes, 'the rates take into account various factors - from the number and nature of the equipment, the activity carried out, the size of the operation (number of clients, number of operations, etc...) and, since there is already a history, also the claims - both of the client itself and of the sector of activity - in which the company operates.'

3

Pedro Figueiredo

Head of Technical Underwriting da Zurich Portugal

1. We know that SMEs represent a large part of the economy and that every investment is carefully thought out. Is this type of insurance recommended for any company with a digital presence, or are there exceptions? In other words, does a Cyber Risks insurance make sense for all companies, or are there cases where it doesn't pay off?

With technological innovation driving the digitalisation of the global economy, and with companies - regardless of their size and sector of activity - increasingly relying on digital technologies for their growth and innovation, cyber risks will pose an increasingly severe threat to companies. The global cost of cybercrime is predicted to increase threefold between 2022 and 2027, to almost 24 trillion dollars.

Being a Small or a Medium-sized company does not equal safety. More and more companies are recognising their vulnerability to this specific risk and protecting themselves with Cyber Risks insurance. Despite this, there are still many companies, especially small and medium-sized ones, which account for around 98 % of our business fabric, which relegate this protection to the background, but which can be seen by cyber criminals as easy targets. It's important to remember that many cyberattacks are often opportunistic.

SMEs sometimes struggle to understand all the risks they are exposed to and the level of protection they need. As such, the insurance market must contribute to the development of solutions that simplify the process of underwriting these insurances and make it possible to cover some of these risks through a standardised solution.

In this sense, since digital threats are constantly evolving and surpass the response capacity of traditional insurance and risk management solutions, we need innovative solutions that mitigate the existing gaps between digital risk and insurability - especially for SMEs - as we have highlighted in the whitepaper Closing the cyber risk protection gap, developed by the Zurich Group and Marsh McLennan“

2. What covers are essential in Cyber Risks insurance to guarantee real protection and return on investment? What should a company expect and demand from a policy in order to feel that it is truly protected?

The insurance sector is able to offer some degree of protection, which is why, as has already been emphasised, it is essential for all companies, given their growing dependence on technology, to protect themselves with Cyber Risks insurance. Some covers that may be important are, for example, civil liability for damage caused to third parties, data recovery due to computer hijacking and loss of profits due to the interruption of the insured's activity.

It should also be recognised that large-scale cyber-events present substantial accumulation risks - which cannot be borne by the private sector.

In this sense, improving companies' cyber resilience and adopting security control mechanisms that reflect best practices in risk mitigation - like ransomware - must take priority. To achieve this goal, solid public-private partnerships are needed to develop comprehensive strategies that guarantee our digital future and resilience against cyberthreats.

After all, it's important to bear in mind that not everything can be insured: there are uninsurable cyber risks, such as the failure of critical infrastructures or the payment of ransoms. Therefore, for anything other than mass malware or mass disruption of cloud access - cyber incidents that are currently considered insurable up to a certain level of financial loss - a public-private partnership will be the answer that can guarantee an effective protection.

The private sector has limited funding capacity and, as the whitepaper concludes, in order to strengthen society and the economy in the event of a catastrophic cyber event, greater public sector involvement is essential.

3. How does one calculate the amount to pay for Cyber Risks insurance? What are the most relevant factors - size of company, area of activity, technological infrastructure, history of incidents?

Just like any other insurance, calculating the amount each company has to pay for Cyber Risks insurance depends on several factors. Larger companies, with a greater volume of data and a higher degree of dependence on digital technologies, may be more exposed to cyberattacks or to more complex attacks, and may therefore face higher premiums. The same goes for companies with a history of cyberattacks, as they are seen as more susceptible to new incidents.

Foto: Kookkii, adobe stock

On the other hand, these amounts can be mitigated when companies show good cyber hygiene practices and invest in employee training on these matters.

Alongside these variables, insurers use risk assessment models that also combine market data and cyberthreat trends. In addition, a personalised analysis is always carried out to understand a given company's specific needs and adjust the policy accordingly.

Finally, it's important to emphasise that the lack of protection against cyber risks is a major issue that needs to be addressed - the threat of cyberattacks represents, as has already been made clear, a significant risk to social and economic stability. And in this scenario, calculating the cost of insurance is not just a technical or financial issue. Rather, it reflects the need for greater collaboration, with the development of innovative solutions, the education and encouragement of insurance buyers and the improvement of the cyber insurance market - so that, once again, our economy and society can be safeguarded.

Managing Cybersecurity Risks in Organisations

The Associação DNS.PT has a course designed specifically to create the skills necessary for participants to be able to safeguard the integrity of their organisation, identify vulnerabilities and plan mitigation strategies in the event of a cyberattack.

Entitled Managing Cybersecurity Risks in Organisations, this free online course is spread over four modules with formative assessment, preceded by an introductory module and ends with a summary module and instructions for obtaining a certificate.

With the increasing digitalisation of services and businesses, the risk of cyberattacks and the compromise of organisations' vital operations is growing. The course covers the process of identifying, assessing and dealing with cybersecurity risks in organisations. In the first modules, the process of analysing and managing risk is presented in detail and, in the last module, participants put their knowledge to the test by answering practical exercises.

Foto: Танюша Коновал, adobe stock

Among other competences, at the end of the course participants can expect to be able to:

- Recognise the main threats and cyberattacks in Portugal;
- Distinguish the concepts of Cybersecurity Risk Management and their process;
- Identify risk scenarios applicable to different types of assets, based on threats and vulnerabilities;
- Recognise implemented cybersecurity controls;
- Assess risks systemically, apply impact and probability criteria and prioritise risks;
- Specify risk treatment options;
- Identify, assess and review risks in a real-life scenario (with a practical case).

Recipients

This course is aimed at all companies and organisations. It aims to equip companies with strategies, methods and techniques to manage cybersecurity risks, explore the different phases of risk management, from identifying, assessing and treating risks, in order to proactively minimise the existing vulnerabilities in organisations.

Anyone can enrol in this course, with no requirement as to previous education or certification. However, in order to have the most positive experience possible, the course organisers advise that participants already have a basic knowledge of cybersecurity.

Enrolment is free, accessible at https://www.nau.edu.pt/pt/curso/gestao-dos-riscos-em-ciberseguranca-nas-organizacoes/ after registration on the NAU platform (also free).

The course lasts 10 hours, but from the moment of enrolment it can be taken at the participant's own pace, according to their availability. At the end, and in order to get the certificate, the participant must have at least 70 % correct answers on all quizzes taken.

The course is available on the NAU platform until 5 June 2026.

Two million .PT registrations

On 9 June 2025, the Bossa Tavira restaurant made history by registering the bossatavira.pt website - the 2 000 000th registration in the .pt domain.

.PT marked the moment with an official statement in which it said that 'this number reflects the internet's dynamism in Portugal and the growing choice of .pt domains by companies, organisations and individuals.'

'*Reaching 2 million .pt domains is a testament to the ongoing work of .PT and its partners to promote the internet in Portugal,*' stated Luisa Ribeiro Lopes, President of the .PT Board of Directors. '*This milestone shows the vitality of our digital economy and the importance of .PT as an online meeting point, where innovation and economic growth come together with the guarantee of an increasingly secure and trustworthy online environment.*'

In addition, a website has also been created, www.2milhões.pt, inviting anyone with a .pt domain to tell their story.

Commission publishes guidelines for providers of AI models

On 18 July, the European Commission published a set of guidelines to help providers of general purpose AI models comply with the obligations of the Artificial Intelligence Act, starting 2 August 2025.

These guidelines clarify the obligations, providing legal certainty for all players across the AI value chain, and complement the General-Purpose AI Code of Practice.

Henna Virkkunen, the European Union's Executive Vice-President responsible for Technological Sovereignty, Security and Democracy, said: 'With today's guidelines, the Commission supports the smooth and effective application of the AI Act. By providing legal certainty on the scope of the AI Act obligations for general-purpose AI providers, we are helping AI actors, from start-ups to major developers, to innovate with confidence, while ensuring their models are safe, transparent, and aligned with European values."

Foto: Anwesha Dey, adobe stock

DNS Abuse Mitigation Report

In response to ICANN's strengthened requirements for 2024 on DNS abuse, the DNS Research Federation (DNSRF) has launched a new initiative to assess real-world compliance and performance.

Using data from the DAP.LIVE platform, this analysis focuses on how effectively registrars and registries are mitigating phishing and malware threats - and how quickly they act within critical response windows.

The full report was published on 3 June.

No More Ransom

The 'No More Ransom' website is an initiative of the High-Tech Crime Unit of the Netherlands Police and Europol's European Cybercrime Centre (EC3), with the support of cybersecurity companies Kaspersky and McAfee, which aims to help victims of ransomware recover their encrypted files without having to pay criminals. The Portuguese National Cybersecurity Centre is also a partner in the project.

Since it's much easier to avoid threats than to fight them once a system is infected, the project also aims to educate users about how ransomware works and what measures can be taken for effective prevention.

At the moment, the website hosts tools capable of decrypting files that have been attacked by several dozen types of ransomware.

2ª edição

Organização

.pt

CURSO
Cód. GRCO

Gestão dos Riscos de Cibersegurança nas Organizações

Salvaguarde a integridade da sua organização identificando vulnerabilidades e planeando estratégias de mitigação em caso de ciberataque.

Descrição

Com a crescente digitalização dos serviços e negócios, cresce o risco de ciberataque e de comprometimento das operações vitais das organizações.

O curso "Gestão dos Riscos de Cibersegurança nas organizações" aborda o processo de identificação, avaliação e tratamento de riscos de cibersegurança nas organizações.

Nos primeiros módulos, apresenta-se em detalhe o processo de análise e gestão de risco e, no último módulo, o formando terá de por à prova os seus conhecimentos respondendo a exercícios de aplicação.

Formato

- Duração: 10 horas
- Esforço: 10 horas
- Ritmo: Ao ritmo do estudante
- Idiomas: Português

O curso distribui-se por um módulo introdutório, quatro módulos teóricos com avaliação formativa e um módulo marcadamente prático. O curso termina com um módulo de síntese e instruções de obtenção de certificado.

Curso

Entre 04/06/25 e 05/06/26

Curso através da plataforma nau SEMPRE A APRENDER

Mais informações em www.pt.pt

This publication is produced by .PT

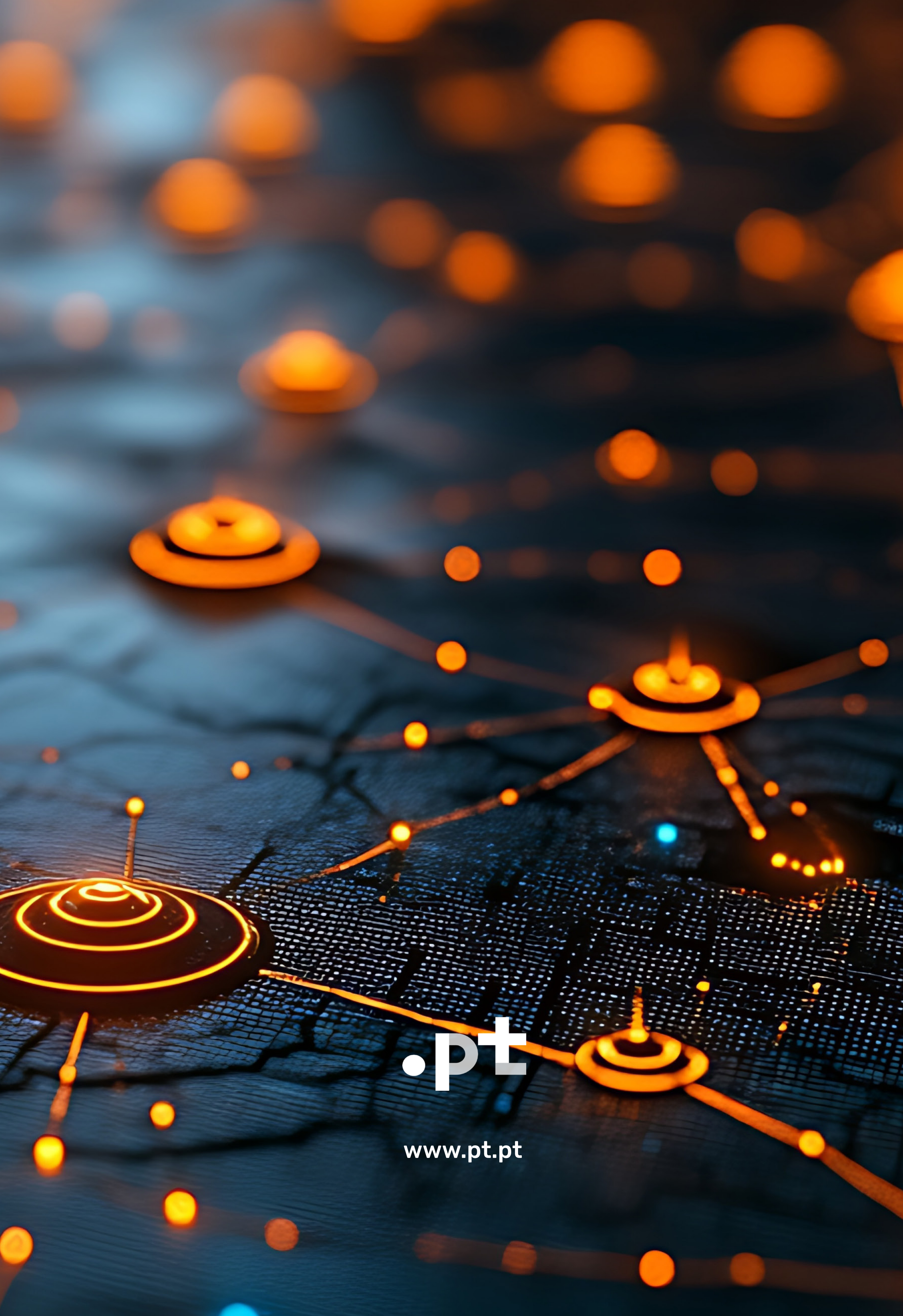
Editor
António Eduardo Marques

Graphic Design
Sara Dias
Maria Cristóvão

Translation
Sara Pereira

Photography
Cover: Nat, adobe stock
Table of contents and back cover: Yesdfg, adobe stock

Quarterly publication
July 2025



.pt

www.pt.pt