
SMEs and the self-employed
Foyer
Cyber Attacks...
protect your data
cyber pro

Do not fall prey to a cyber criminal

For you as a business owner or a self-employed individual, IT systems (email, data storage, computer servers, the internet, etc.) play a large role in your business activities. They make your business easier to run, and constitute a major source of often sensitive data that has to be protected.

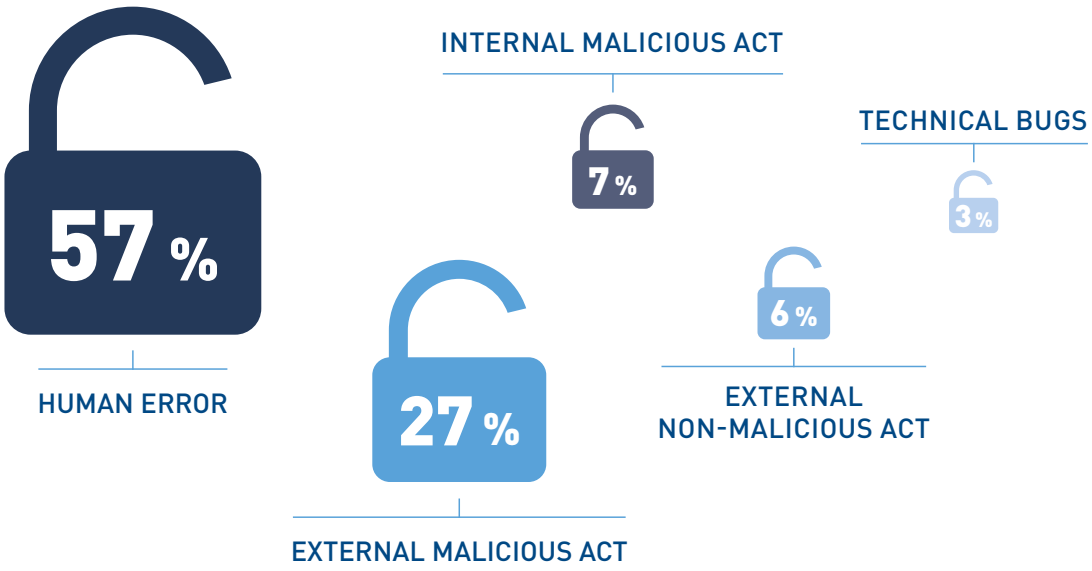
You are probably aware of terms such as cyber-attack, phishing, ransomware, trojan horse, malware, spyware or dark web. They represent a real threat to your business as regards **cyber crime**.

What do you do if you find yourself facing a situation where there has been a leak of personal, confidential data, or your payment system is hacked, or all the data crucial to your business is encrypted, or if a mistake by an employee means protected data is sent to the wrong recipients?

You are an ideal target for cyber-criminals, regardless of your area of business or your size; the information and data you hold are bound to attract attention.

You will understand that for your business to run smoothly, **you should do your utmost to prevent such attacks**.

Data **breaches** CNPD Annual Report 2018



The **risks** run

Total data loss (e.g.: estimates, invoices, orders, customer data, etc.)

Disclosure of confidential data (e.g.: patients' medical records, customers' bank details, etc.)

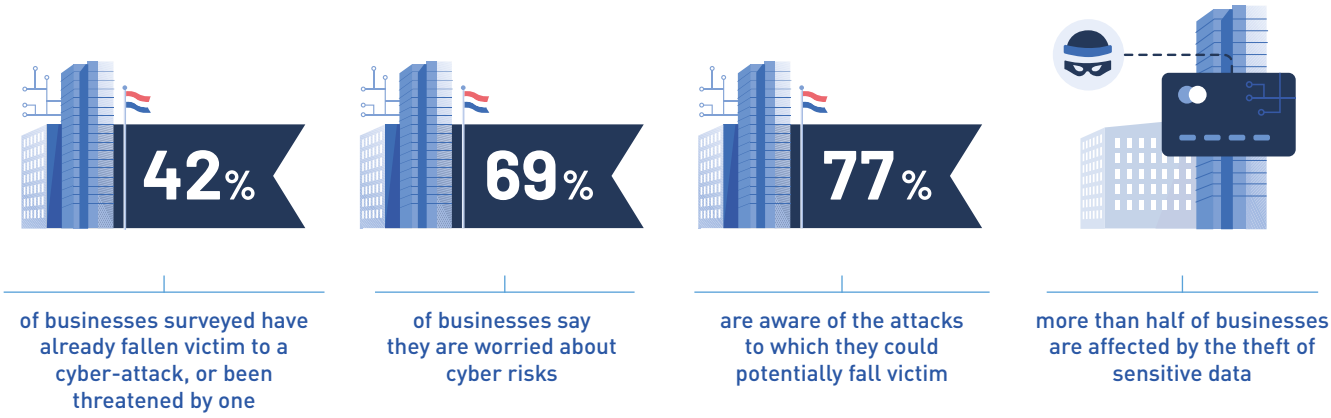
Business interruption and therefore **lost revenue** (e.g.: temporary inability to access computer servers)

Serious financial penalties in the event of a breach in data protection regulations. All businesses are obliged to inform the relevant authorities and the people concerned (such as customers) about any personal data breach.

My laptop was stolen from my office. It contains the medical records of more than 800 patients, some of whom are well-known people. I am very worried about the consequences this incident might have on my reputation.

My computer was hacked. All my business data including my plans, estimates, purchase orders and invoices have been encrypted. The cyber-criminal is demanding a $ 5,000 ransom, in bitcoins, to send me a decryption key. I might lose a major project in progress.

As Luxembourg's leading insurer, Foyer Assurances in conjunction with the Ministry for the Economy, conducted **market research** about your concerns and requirements as SMEs and self-employed business people. A few of the highlights are:



of businesses surveyed have already fallen victim to a cyber-attack, or been threatened by one

of businesses say they are worried about cyber risks

are aware of the attacks to which they could potentially fall victim

more than half of businesses are affected by the theft of sensitive data

WHY TAKE OUT INSURANCE?

- To be able to **react quickly** if there is a breach
- To ensure **business continuity**
- To **receive help from professionals**. You can rely on their skills, leaving you to focus on continuing to run your business.
- To receive guidance on **meeting new regulatory obligations regarding data protection**
- To **protect your reputation** by limiting the negative impacts of an attack and maintaining your customers' trust

The server used by my online sales company was attacked and we haven't been able to sell anything for several days. The impact on my turnover has been disastrous. If I don't find a solution quickly, I could go bankrupt.

My bank has just told me my payment terminal was hacked by malware on a very busy day. Several hundred customers' bank details are available to cyber-criminals. What should I do?

The Foyer solution - **cyber pro**

It is aimed at the self-employed and small and medium-sized businesses with turnover under € 10 million. The service naturally includes **an insurance component**, but importantly **an assistance component** to support and guide customers through emergency situations.

FOYER WILL HELP IN CRISIS MANAGEMENT, AND TAKE CHARGE OF:

- **Identifying** and confirming the nature of the problem
- **Advising** on actions to take and statements to issue
- **Analysing** the seriousness of the threat
- **Notifying** any victims
- **Negotiating** with cyber-criminals
- **Removing** viruses
- **Online intelligence regarding** the stolen data

Managing IT-related incidents requires responsiveness, support and expertise.
Foyer has consequently joined forces with partners able to meet those challenges.

ASSISTANCE HOTLINE NUMBER, 24 HOURS A DAY, 7 DAYS A WEEK : 437 43 3100

FOYER COVERS THE LOSS AND HARM SUSTAINED BY YOUR BUSINESS AND/OR CAUSED TO THIRD PARTIES

- All the costs incurred to **investigate and remedy** the threat
- Ensuing gross **margin lost**
- Spending on **business continuity**
- Costs charged to insureds by the **issuers of bank cards**
- **Investigation** costs paid by insureds charged by the CNPD (France's National Data Protection Commission)
- **Compensation claims** by third parties (users and/or banks)
- Costs incurred on **repairing the reputation** of the business
- **Civil liability** claims
- Civil liability claims in connection **with website content**

Calculate your risk online on the Ministry for the Economy website by taking the cyber-security evaluation questionnaire and **receive a 10% discount** on your insurance (https://startup.cases.lu/)

Would you like to insure your business against these risks? Delay no longer - contact your Foyer agent or visit foyer.lu in the section Professional.

CYBPRO-082022-EN

Foyer

Einfach fir lech do

Foyer Assurances S.A.
12, rue Léon Laval - L-3372 Leudelange
R.C.S. Luxembourg B34237

T. 437 43 44
www.foyer.lu