June 2020

+ Cyber security lexicon for SMEs

Mission ‘peace of mind’

Investigation Report cyber security at Belgian SMEs

It just takes
one mailicious email

proximus
enterprise

Contents

Introduction

Year-on-year, the number of cyber-attacks is increasing worldwide. SMEs are also increasingly being affected by cybercrime.

*International research agencies regularly study the cyber security landscape. But, for Belgian SMEs, their figures are not always representative. This is the reason why Proximus organised two studies of its own: a qualitative and a quantitative investigation at **122 Belgian companies.***

3 key facts from the investigation:

1. **Nine out of ten** Belgian SMEs are concerned about possible.
2. **Phishing** attacks are the most common.
   One in four malware attacks concern ransoms.
3. Belgian SMEs are very **heterogeneous** in how they approach their security.

Methodology

Target group

The SMEs surveyed had 25 to 250 employees and came from a variety of sectors with the exception of ICT services.

Respondents

The respondents were CEOs, CIOs and other decision-makers.

Data collection

A mix of qualitative 60-minute face-to-face in-depth interviews and an online survey.

Sample size

122 Belgian SMEs participated in the qualitative and quantitative investigation.

- 63% from the Flemish Region
- 29% from the Walloon Region
- 8% from the Brussels-Capital Region

Investigation period

Proximus examined the cyber security of Belgian SMEs in the period from November 2019 until February 2020.

‘You can install as many security applications as you like. But if users don’t use their common sense then there is little point.’

respondent a

Investigation results

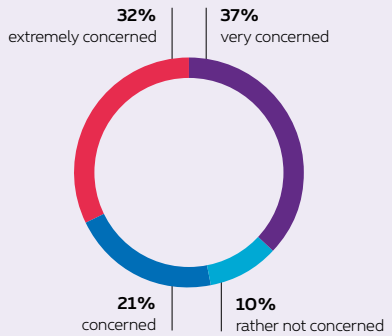
Cyber security = top priority

SMEs are often less well protected than larger companies, but they have just as much sensitive data such as customer data about people or businesses, intellectual property rights, etc. **In 2018, the damage caused by cyber attacks against Belgian SMEs increased by no less than 194 (!) percent,** Vanbreda Risk & Benefits quantified in its Cyberstudie 2019.

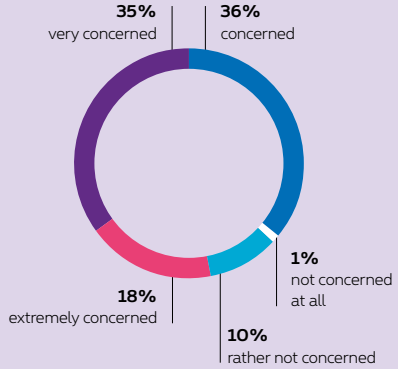
- All respondents indicated that cyber security is a **top priority**.
- The most common security risks that the respondents see are **users** and **mobile devices**.
- Belgian SMEs are very worried about **data security** (data leaks) and **business interruptions** (business continuity) as a result of cyber attacks.

Nine out of ten SMEs are concerned about being attacked. It is striking that SMEs that have already experienced a cyber attack in the past, are more concerned about a new attack than SMEs that indicate that they have not yet been attacked.

How concerned are you about the possibility of again becoming a victim of a cyber attack?



How concerned are you about becoming a victim of a cyber attack?



One in five of the Belgian SMEs surveyed was affected.

Number and types of attacks

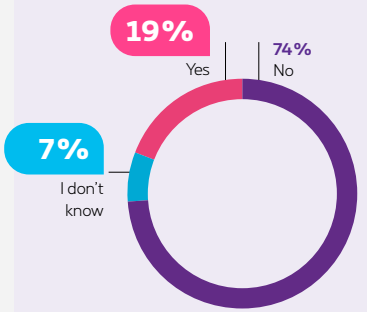
At the beginning of 2020, a number of Belgian companies were brought to a stand still for several weeks because of a cyber attack. Fortunately, not every attack is so drastic. The American Ponemon Institute calculated that **56% of the SMEs in the Benelux experienced – knowingly or not – a cyber attack in 2019.**

One in five of the Belgian SMEs surveyed was affected.

- **19 percent** of Belgian SMEs indicate that they were **victims** of a cyber attack in 2019.
- **7 percent** (!) of the SMEs surveyed **did not know** whether they were attacked or not.
- Of the SMEs that indicate that they have not been attacked, only 22% are very sure about this. (20 percent answer that they are not sure.)
- Also striking: 16 percent of the respondents are not sure how long the attack had been going on before they discovered it.

1. That is far less than the 56 percent from the Ponemon Institute study. It is possible that the Belgian SMEs were not hindered by the attacks or even that they were not aware that they had been attacked.

Has your company been the victim of a cyber attack in 2019?



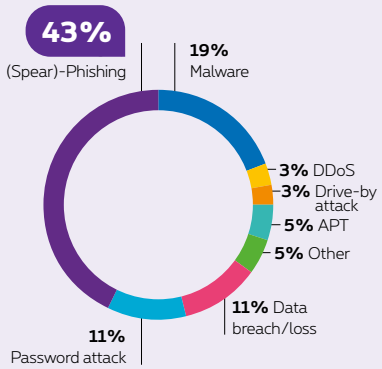
Many phishing but also malware attacks.

- **Phishing** is the most common type of attack with **43 percent.** This is followed by **malware (19%)** and **password hacks (11%).**

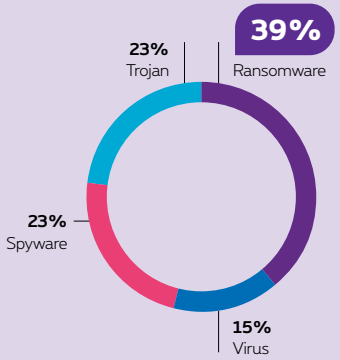
- **Four malware attacks in ten** involve a **ransom**.

To prevent phishing and ransomware, the security of your employees' **mobile devices** (smartphones, tablets, laptops) is an essential part of your security strategy. On a smaller screen, often with a simplified graphical information display, employees are even more likely to click on an unreliable url and hackers have got one foot in the door. At the very least, combine a mobile device management platform that offers Threat Protection with sufficient training and awareness-raising for your employees.

What kind of attack was it?



If malware, which malware?



‘Data theft is a nightmare. Sometimes I can’t sleep because of the possible consequences.’

respondent b

‘I can’t even think about shutting everything down. That would cost you thousands of euros per hour.’

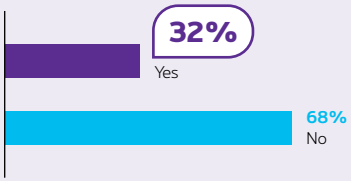
respondent c

Major consequences

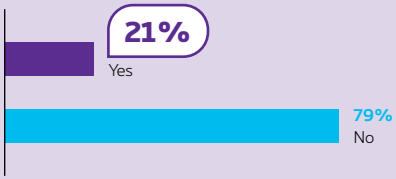
A cyber attack can have far-reaching consequences for businesses. The insurance company Hiscox calculated that the **average cost** of cyber attacks on Belgian companies in 2019 amounted to **441,000 euros** (486,000 dollars).

- **32 percent** of respondents indicate that their employees were **unable to work** because of the cyber attack.
- **21 percent** of respondents lost **company data** or company data was made inaccessible.

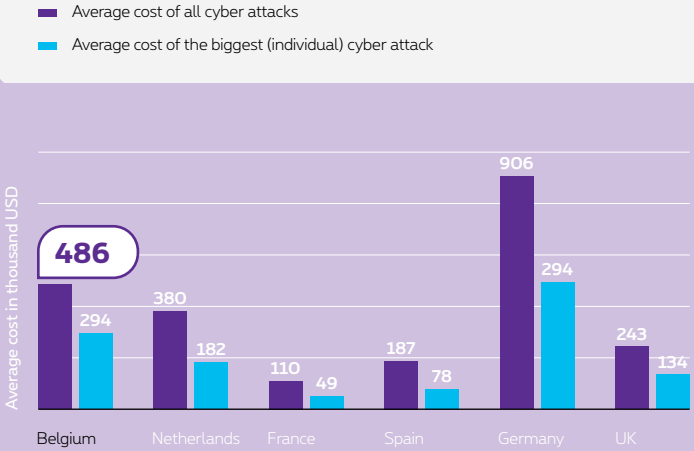
Was the attack such that your company’s employees could no longer work?



Was data lost or made inaccessible?



486.000 dollar. That is the average cost of all cyber attacks on Belgian companies in 2019.



Source: Hiscox report, conducted by Forrester Consulting, 2019

Security approach

A firewall, no encrypted hard drive

Most SMEs have a solidly secured front door, but a prudent owner goes a lot further to prevent unwanted guests. Which security solutions do SMEs choose to keep things **secure** but in an **affordable** way? A lot of smart solutions can protect your ICT infrastructure without needing major investment.

How do you protect yourself?

Almost always implemented

- firewalls
- backups
- antivirus

Sometimes implemented

- spam and reputation filters
- advanced threat protection
- wifi guest network

Rarely implemented

- managed security system
- Multi-factor authentication
- encrypted hard drives
- proxy server
- ethical hacking
- cyber insurance

‘I’m not a computer scientist at all and sometimes I have little time for it, but cyber security is one of my responsibilities.’

respondent d

Many do-it-yourselfers

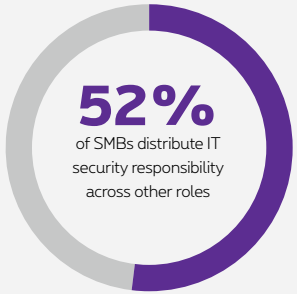
ICT knowledge and trust in external partners determine how an SME regulates its cyber security.

SMEs organise their management and monitoring of their security environment in very many different ways.

- 41 percent manage and monitor their security infrastructure entirely **themselves**
- One third of SMEs divide security tasks between **their own employees** and an ICT **partner**.
- A quarter of SMEs outsource the management to an **ICT partner**.

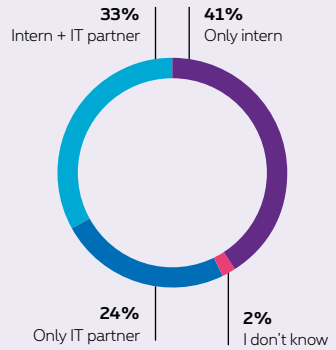
Fragmented responsibility

At slightly more than half (52%) of the SMEs, responsibility for cyber security is shared across different profiles within the company.

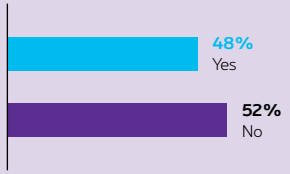


source: Untangle 2019 SMB IT Security Report

Who monitors and manages your security infrastructure?



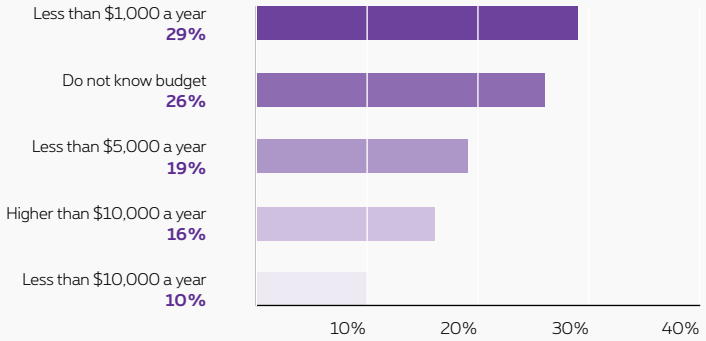
Is there one designated person responsible for cyber security within your SME?



Modest budgets

29 percent spend less than 1,000 euros a year on cyber security.

What is the budget that your SME spend annually on cyber security?

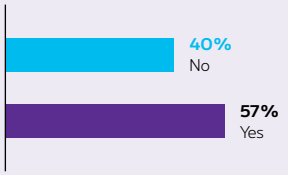


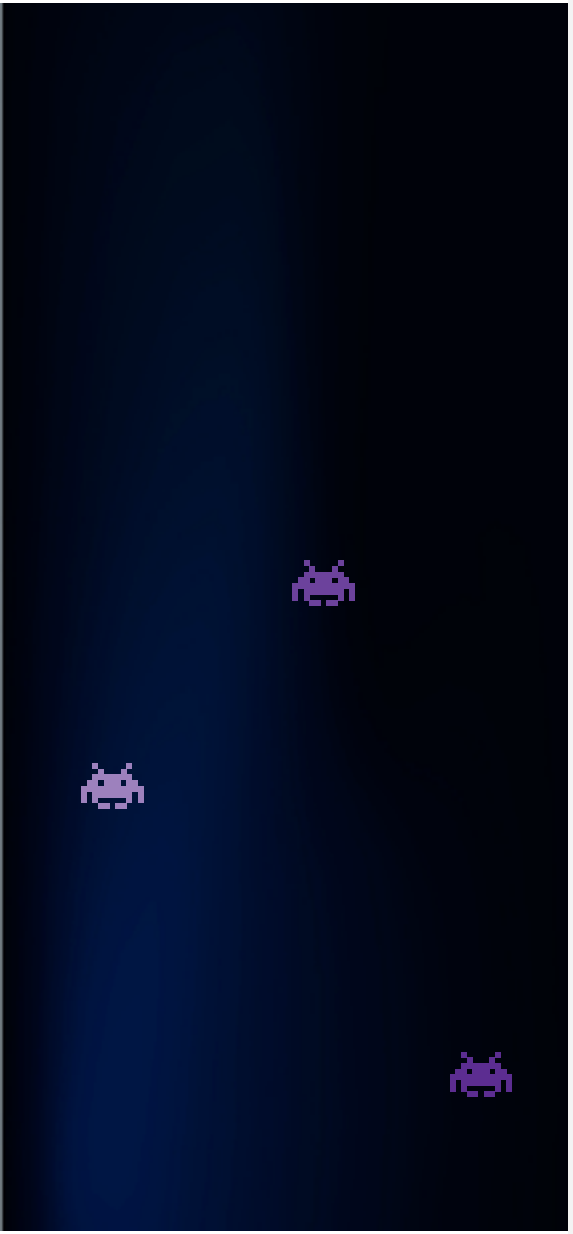
source: Untangle 2019 SMB IT Security Report

One SME employee in three does not receive security training

A chain is only as strong as its weakest link. A company may have a sophisticated alarm system, but if an employee forgets to close the back door, this has little impact. **Human activity** is the **weakest factor** in cyber security. Raising employees' awareness of cyber risks is an essential part of any security approach.

Do your employees receive training on how best to handle your company's digital devices and data?





Secure your business in 4 steps

And you? How do you create your plan for peace of mind?

1. Determine your profile

Choose what is critical and what is less critical.	› For each part, weigh the security costs against the possible impact of an attack.
List the **critical operations** and **vital assets** that you need to protect.	› Which **systems, networks, ICT devices, ICT applications and data** are essential for your business? › Make an inventory of all **offices** and **devices** that you need to protect. › Identify which **employees should and should not have access.** › Also consider **physical security**: make sure, for example, that not every visitor can just walk into your server room.
Decide what you want to do **internally** and what you want to do **externally**. Do you have sufficient know-how and manpower to follow up on everything yourself? Think about:	› the design and implementation of your security infrastructure (see below) › follow-up and incident management (see below) › tests and training (see below).

2. Design and set up your security

- **Design** either yourself or with a partner your entire 360° security infrastructure. Map out, for example, how you can split up your internal network in the most optimal way. Between which networks do you need to place additional firewalls? Who has access to what? Do not forget to include an e-mail security system, even if you have Office 365. Multi-factor authentication and a good back-up strategy should also be included.
- Prepare a **step-by-step** plan for the implementation of new infrastructure. Bear in mind that for some installations you will have to interrupt your service.
- **Document** all settings, serial numbers, software and hardware versions, locations in the building, cables etc.

3. Follow up and create an incidents plan

- Prepare procedures for following up alerts **7 days** per week and **24 hours** per day.
- Have someone regularly review the **status** and **logs** of your security solutions.
- Record beforehand what you are going to do in the event of an incident. **Who responds, how quickly, with what resources?** Who will notify you? Who has ultimate responsibility?

4. Test, train and book success

- Organise an exercise case to test your incidents plan.
- Train employees to use your infrastructure intelligently.
- Enjoy peace of mind, thanks to 360° protection and further develop your business.

The customised offer from Proximus

Find out about the 360° approach that Proximus takes for the cyber security of your SME. Choose yourself what you want: from full care to specific security services.

A sound basic security does not need to be expensive.
Take our 360° approach:

Predict

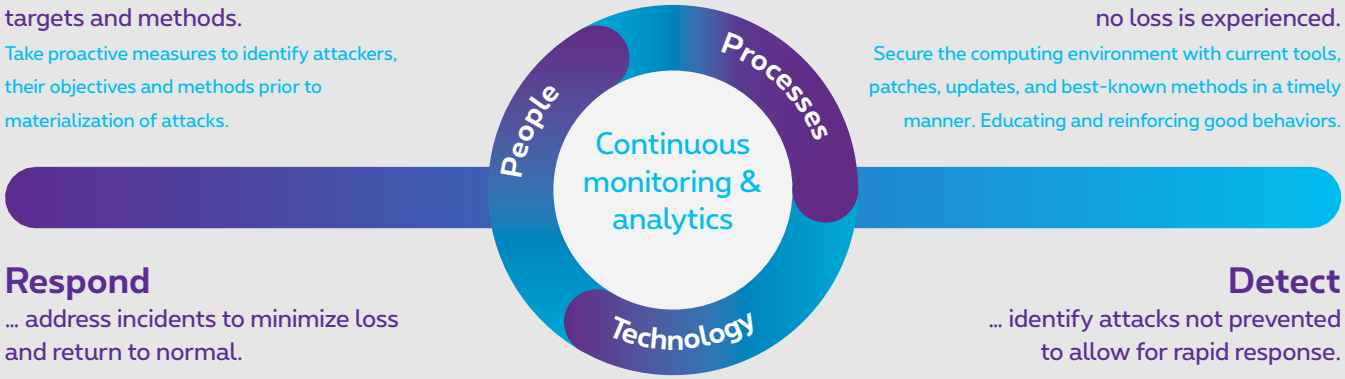
... the most likely attacks, targets and methods.

Take proactive measures to identify attackers, their objectives and methods prior to materialization of attacks.

Prevent

... or deter attacks so no loss is experienced.

Secure the computing environment with current tools, patches, updates, and best-known methods in a timely manner. Educating and reinforcing good behaviors.



Respond

... address incidents to minimize loss and return to normal.

Manage efforts efficiently to contain, repair and recover as needed, returning the environment to normal operations.

Detect

... identify attacks not prevented to allow for rapid response.

Monitor key areas and activities for attacks which evade preventions. Identify issues, breaches and attacks.

Audit or improvement phase. We analyse your approach and propose actions to improve your security.

Consultancy and design. We provide advice and design a secure digital environment for your business. We identify the risks and costs and, together, we map out your security policy.

Follow-up and advice. Our security consultants monitor your digital environment and regularly evaluate your security reports. They formulate advice and suggestions for improvement.

Customised solutions that we can implement for you:

- Network security solutions, such as state-of-the-art firewalls, network access control and web security.
- Advanced Threat Protection solutions, such as intrusion prevention systems, DDoS protection, advanced malware protection and SSL encrypted traffic visibility.
- Web application firewalls, XML gateway, prevention of data loss, e-mail security and strong authentication.
- Endpoint protection solutions that provide protection for (mobile) endpoints and (virtual) servers
- 'Managed Security Services': remote services to monitor and manage the most important security components of an IAS (Internet Access Street) or data centre.
- Remote Operations Centre (ROC) that monitors the latest threats 24 hours per day, 7 days per week and intervenes proactively if necessary.

YES,
I would like an exploratory discussion

Bronnen

www.proximus.be
www.ictportal.nl/ict-lexicon/cybersecurity-woordenboek

Proximus & cyber security

The Proximus group is the market leader in Belgium for telecom & IT services. The group operates in the Benelux and serves residential customers, businesses and public services. Proximus strives to guide companies on their path to digital transformation by combining the best connectivity resources (e.g. fibre, 5G, etc.) with expertise in domains such as Cloud, the Internet of Things (IoT), Big Data and Cyber Security in order to come to solutions with a decisive impact.

Proximus is a trusted partner in helping to develop and implement a balanced security strategy.

› Together with its affiliates, Proximus has more than 350 employees specialised in cyber security.

- Davinsi Labs
- Spearit
- Telindus Luxembourg
- Telindus Nederland

› Proximus has over 20 years of experience in cyber security:

› Proximus is a member of various cyber security associations for exchanging best practices: Cyber Security Coalition, ETIS, Beltug, etc. This means we are always aware of the very latest developments. We use this knowledge to provide even better protection for our customers.

Want to know more?

Visit www.proximus.be/security or contact one of our security experts.

Cybersecurity-lexicon

Whether or not you monitor the cyber security of your SME yourself: with the help of these 25 security terms, you can better protect your business. Talk to internal or external security specialists and take your peace of mind to a higher level.

1. **Advanced Threat Protection** (ATP) Software that provides protection against unsafe attachments and harmful links to unsafe websites.

2. **Audit log** File that records what has been done in your computer system, by whom and when.

3. **Bot** A computer programme that can perform tasks independently. Bot is an abbreviation of robot.

4. **Captcha** Abbreviation of "Completely automated public turing test to tell computers and humans apart". A method for checking whether the user is a human being.

5. **CEO/CFO fraud** A form of fraud in which an attacker sends emails to a financial department in the name of a company's CEO or CFO. The attacker wants to convince or pressure an employee to transfer money.

6. **Cloud Access Security Broker** (CASB) A security solution for cloud applications in which a secure link is placed between the company network and the cloud.

7. **Cyber insurance** Insurance covering financial loss as the result of a cyber attack. The insurance pays not only for damage incurred by the organisation itself, but also for damage that you have to compensate to others.

8. **Distributed Denial of Service** (DDoS) An attack in order to make a service unavailable by flooding a server, application, network, etc. with useless data traffic.

9. **Firewall** A collection of computer programmes or equipment that protect a network.

10. **Insider threat** A threat that originates within the organisation. For example, because employees,

former employees and suppliers can access information.

11. **Managed security service** Remote management and monitoring of a company's security environment by a third party.

12. **Multi-factor authentication** A method for determining whether a user or digital system is who or what he/it claims to be. You can use different methods for this. For example, a password and a code that the user receives via a text message.

13. **Mobile device management** (MDM) Ensures mobile devices are properly managed and secured within an organisation. For example, by setting a pin code for smartphones and tablets. Or by ensuring that you can remotely erase data on those devices.

14. **Network access control** A way of ensuring better protection of a network by allowing only known and authorised devices on the network.

15. **Phishing** An attack whereby the attacker entices someone to provide important information, such as login or credit card data. Phishing is often done via e-mail, but also via phone, text or another message.

16. **Privacy Impact Assessment** Process by which an organisation gains insight into the privacy risks.

17. **Ransomware** Well-prepared attack in which data is encrypted or made inaccessible. The attacker promises you a key to "free" your data in exchange for a "ransom".

18. **Remote Operations Centre** A department that monitors the latest threats 24 hours per day, 7 days per week. This allows it to respond quickly and proactively to avert risks.

19. **Role based access control** Determines whether a user may access a computer system. This is done based on the role that the user or a group of users has. Examples of roles are viewer, editor and manager.

20. **Rule-based detection** Method of detecting a cyber attack. You determine beforehand which patterns or indications in the data on a network may be suspicious. The system then searches for those patterns or indications.

21. **Sandbox** Screened-off part in a digital system. Software that operates in this location cannot interfere with other processes on the computer. A sandbox is used to run software that is often compromised. Or to test if something is malware and what it does.

22. **Single sign on** (SSO) End users log in once and can then work in different applications and parts of the network. They therefore no longer need to enter login details each time.

23. **Spam filter** Software that tries to recognise and remove spam and computer viruses.

24. **Spoofing** The attacker hides his identity or presents himself as another user / someone else (masquerading, source routing).

25. **Spyware** A form of Malware. Spyware is software used to collect and transmits information in an unnoticed manner. These are often keystrokes, screenshots, e-mail addresses, browsing behaviour or personal information such as a credit card number.

Sources

www.proximus.be

www.ictportal.nl/ict-lexicon/cybersecurity-woordenboek


proximus
enterprise