SPARRING CAPITAL

EDITORIAL

CYBERSECURITY

Two out of three. That is the number of French companies believed to have faced a cyberattack in 2018. While this risk was seen for many years as an issue only for large firms, cybersecurity is today a major challenge to the entire fabric of the economy, particularly because SMEs and intermediate-size firms are often less well protected than large groups although they hold critical information. As an aggravating factor, they often have less capacity to respond effectively to malicious acts and therefore any serious attack can have a lasting impact on their operations.

Protection of company information systems is achieved through the application of an approach based on a number of key points such as implementing a prevention plan, building and testing a backup system, establishing a rapid reaction force and taking out an insurance policy.

We wanted a deeper understanding of this subject and we have therefore included a joint interview with Lari Lehtonen (in charge of the "cyber risk" team at Marsh France) and Jean-Francois Louâpre (cybersecurity expert) in this autumn newsletter.

We hope you enjoy the reading!

The Sparring Capital team

PORTFOLIO NEWS

Acquisition of Cesacap

In April, Sparring acquired Cesacap, a major player in electrical engineering in the Paris area, from Capzanine, SG Capital Partenaires and the group's founders as part of its transfer to a new management team.

Founded in 1981, the Cesacap group has expertise in high and low voltage, with a strong presence in Ile-de-France. Cesacap is able to support its customers on all sizes of projects, including renovation and new build. The group also benefits from a varied range of activities, and in particular is well known in the tertiary sector (Cesa), social housing (Perrin) and new residential development (Meusnier).

The group generated sales of around €50 million in 2018, with 250 employees. It has undergone solid growth in recent years under the leadership of Franck Petit, its President, who has reinforced the staff, notably with the arrival of Fabrice Gaté as Chief Executive Officer in 2017. Growth is based on both the group's well-established know-how and its managed diversification policy.

An ambitious development plan has been drawn up by all the project partners to pursue the strategy of organic growth while relaunching the group's external growth policy.

Acquisition of Softair by Cesacap

Four months after its acquisition by Sparring Capital, the Cesacap Group (renamed Weecap in the summer of 2019) completed its first external growth operation by acquiring Softair, a company specialising in HVAC engineering.

Softair is involved in the installation, maintenance and repair of heating, ventilation and air conditioning equipment. The company operates mainly in Ile-de-France on non-residential building renovation projects and generated more than €10 million in revenue in 2018.

Thanks to this merger, the Group is diversifying its service offer and benefiting from commercial and operational synergies, such as positioning on calls for tenders combining electrical and HVAC engineering packages (a first joint project has already been won by the teams), additional services offered to the customers of each of the two companies and the opening up of new types of projects.

Acquisition of Nalys

Sparring Capital is expanding internationally with the acquisition of Nalys, a Belgian engineering consulting group.

Created in 2011, the group is undergoing strong and sustained growth, thanks to its expertise in recruiting staff with relevant profiles and the setting up of an internal training institute. Nalys targets both large accounts and SMEs, mainly in the fields of Healthcare and Embedded Systems.

With more than 220 consultants, the group has a turnover of more than 23 million euros and intends in the coming years to continue its organic growth in Belgium and develop in France where it now generates 10-15% of its turnover.

This operation allowed the exit of two of the three founders, while the founding director Patrice Serange, former director of Alten Belgium, increased his stake in the company.

INTERVIEW

Lari Lehtonen **is the head of the "cyber risks" team at Marsh France.**

Jean-François Louâpre **provides advisory and training services in cyber security. Previously Information Systems Security Manager for CNP Assurance and AG2R La Mondiale, Jean-François now works with smaller companies, mainly in the financial**

sector.

Can you give us an insight into the extent of the "cyber" risk for companies?

Lari Lehtonen: *"Around two out of three French companies faced an attack on their IT systems in 2018. Even though this type of statistic is difficult to confirm, we are seeing a significant increase in the use by companies of "cybersecurity" insurance every year, with an increase of 70% between 2017 and 2018 and in 2019, a level equivalent to the full year 2018 was reached at the end of June.*

The top three insurance claims are (1) "ransomware" attacks with an attempt to extort money in return for restoration of access to data (2) "denial of service" attacks that lead to a computer server going offline and (3) leaks of personal data, whether malicious or accidental."

Jean-François Louâpre: *"According to a study published by CESIN[1] at the beginning of the year, about 80% of the 200 largest French companies suffered an attack in 2018. I agree with the figure mentioned by Lari.*

Indeed, larger small and mid-cap companies are becoming increasingly attractive targets for cybercriminals because they are generally less well prepared and protected than the large-cap companies, while still having very interesting data. There has also been a spate of attacks on smaller companies with the objective of using them as a "gateway" to penetration of the IT systems of the larger companies with whom they may have business relationships."

[1] Club des Experts de la Sécurité de l'Information et du Numérique (Club of Information and Digital Security Experts).

In your experience, what are the consequences for the companies concerned?

Lari Lehtonen: *"The first consequence is organisational, with financial consequences following very rapidly, whether from business interruption caused by inability to produce or sell due to an IT system failure, or costs incurred in restoring both the IT system and any data that may have been corrupted.*

The costs to companies which undergo these attacks are very variable, depending on the size of the companies concerned and the type of attack. Generally, they range from a few tens of thousands of euros to several million euros. However, it is reasonable to consider that for a larger small firm or mid cap, the cost can rapidly reach several hundred thousand euros. In our experience, a ransomware attack impacts activity for an average of 3 weeks. In some cases, the effects of the attacks have lasted up to 9 weeks before a return to the nominal situation."

Jean-François Louâpre: *"I agree. It sometimes takes weeks or even months to return to a normal situation. In terms of the consequences, it is worth noting that financial issues are just a part of the problem. The reputational issue is at least as important because a massive attack results in a loss of trust from the company's partners: loss of consumer confidence in the event of theft of personal data or loss of trust from commercial partners if the attack allows third parties to access sensitive intellectual property or even their own systems. We also notice that calls for tender are increasingly often asking for information about the security of information systems."*

What are the key principles SMEs and intermediate firms should adopt to protect themselves effectively?

Jean-François Louâpre: *"Above all, it is important to stop saying "This does not affect me" or "it is too complicated". As we have said in the first part of our interview, all companies are now affected, not least because some attacks, such as ransomware, do not specifically*

target a company but instead have the objective of reaching the largest possible number, as was the case with Wannacry.

In relation to the level of complexity associated with IT protection, I would encourage company managers to obtain the ANSSI - CPME[2] guide, which includes what can be called "basic rules of good practice" in IT. The measures set out in this guide are simple to implement, apply to all companies and significantly reduce the risks. The most mature companies can also apply the most relevant measures from the 40 rules recommended by ANSSI[3].

However, a company can only limit the probability of risk because, in relation to IT security, there is no zero risk. That's why it's important to go beyond prevention and prepare a safety plan for the day a problem occurs."

[2] "Guide des bonnes pratiques de l'informatique" (Guide to Good IT Practice) by the French National Cybersecurity Agency and the Confederation of SMEs
[3] Guide d'hygiène informatique

What exactly does such a "safety plan" consist of?

Jean-François Louâpre: *"A safety plan includes, on the one hand, the preparation of an "operational response plan" to be implemented following an attack and, on the other hand, the arranging of insurance cover. Lari will provide more detail on this as it is an essential dimension of the safety plan. Preparation for a possible attack can be broken down into two main components: the response to the attack itself and the implementation of the continuity plan.*

Regarding the response to the attack, the key is to have identified experts in advance, so that they can be called in as soon as possible if a problem arises. To enable the company to make the best decisions quickly, limit risks and avoid knock-on effects, you need to use a cybersecurity expert, but you need to know who call when the problem occurs! The French government "Cyber Malveillance" initiative on assistance and prevention of digital risks, aimed at SMEs, professionals and individuals, is a real step in the right direction and facilitates the relationship with the experts[4]. It's also important to have support from legal and communications professionals when the computer attack affects or risks affecting the company's partners, whether it involves the theft of personal data or access to sensitive documents. In relation to this, it should also be noted that some commercial contracts include information obligations in the event of an incident, as does the GDPR[5] legislation.

When drawing up the continuity plan, it should make it possible to ensure, at a minimum, that data backups cannot also be attacked and have been tested "cold". Finally, it is necessary to train the staff so that organisation of the resumption of activity is as fluid as possible when the time comes."

Lari Lehtonen: *"While it is important to invest in cybersecurity, as Jean-François has pointed out, this does not exclude risk, and insurance is therefore the cornerstone of the safety plan: cybersecurity reduces the frequency, but the intensity remains the same. Finally, as in the case of a company protecting a building with sprinklers, the system limits the occurrence of fires, but no one would consider cancelling their fire insurance policy. Thus, cybersecurity goes hand in hand with insurance.*

Cyber insurance has three main aspects. First, prevention: this can involve phishing tests, intrusion tests, incident preparation, etc. It is something that tends to develop. The second aspect concerns the assistance provided to the company during the cyber event: insurers provide a hotline from which companies affected by a cyber event can obtain the help of a range of experts (IT, legal, and crisis communication). The objective is to manage the event as quickly and efficiently as possible and give the company all possible means to get back on its feet as soon as possible. Lastly, the third and final aspect is based on compensation, which includes the usual insurance mechanisms.

It is worth noting that cyber risk is not generally covered by the insurance policies usually taken out by companies. Cyber insurance covers business interruption caused specifically by a malicious attack on or an accidental event in the company's information systems, together with all costs and any claims related to the event. In summary, this insurance

covers damages suffered by the company and by third parties as a result of a cyber event in the company's information systems.

Turning to the costs associated with setting up such an insurance policy, each case naturally needs to be considered individually, but let us say, as a general illustration, for a company with a turnover of €50 million the annual cost of cybersecurity coverage with an upper limit around €1 million is in the order of €5,000 to €7,000 per year."

(4) List of experts on the website https://www.cybermalveillance.gouv.fr/annuaire-des-specialistes/
(5) General Data Protection Regulation