Contents

Introduction

Pierre Bessé

***Hugo Ronsin**, Boury, Tallon & Associés*
Welcome to this live discussion on cyber resilience, organised by Bessé. We are currently witnessing an explosion of the cyber risk: the number of attacks has quadrupled in France this year, and the improvement of our cyber resilience is a matter of urgency. This discussion will focus on two areas: the impact of a possible cyber crisis on the value of our businesses, and the insurance solutions to improve cyber resilience. Here is Pierre Bessé, CEO of Bessé, to open this discussion.

"This is an "overly-frightening" world, in which cyber threats are omnipresent."

PIERRE BESSÉ

"I hank you, and welcome everyone. We debated the pertinence of organising this meeting, but current headlines prove just how necessary it is: every day, pharmaceutical laboratories, ship owners and hospital websites come under attack. "This is an "overly-frightening" world, in which cyber threats are omnipresent." Furthermore, digital technology just keeps evolving, one recent illustration being the stock market launch of Coinbase, a virtual platform for trading totally dematerialised cryptocurrencies, which achieved landmark valuation. The omnipresence of this virtual world and its associated risks force us to find ways of coping, as we have also had to do for the health risk.

We have been working on the topic of cyber risk for more than 6 years. We have published three studies and partnered the world's best experts – ANSSI (France's cyber security agency), FIC (international cybersecurity forum), etc. – and I would love to be able to say that we have truly raised awareness, enabling us to work together to design specific solutions to counter this danger. However, although the French President has launched a plan with a budget of €1 billion to invest in this field, this is little compared with the €430 billion spent on fighting the health crisis, and certainly not enough to face the dangers of the cyber world. The creation of a campus in Paris is a very good idea, like many other private initiatives that are taking shape -and in which we are often involved-, along with contributions from Institut Montaigne and other leading organisations. I was also rather astonished to learn that Jerome Powell, Chairman of the Federal Reserve of America, believes that the cyber risk is the main risk facing the world economy, with potential consequences that could be even more severe than those of the 2008 crisis, notably in the hypothetical case of an attack on payment methods and financial transactions. I hope that I will be believed, as we could have believed Bill Gates in 2015 when he claimed that a pandemic could threaten the world, and I sincerely hope that we will develop ways of finding essential solutions. Are businesses aware of this urgency?

"We must work upstream, because insurance can only be one element of a much larger set of solutions, including risk identification and the organisation of our response."

PIERRE BESSÉ

I would say so, because they feel more concerned, but much still remains to be done.

We must therefore make proposals that are not limited to insurance, because the world of off-the-shelf products -with policies whose exact coverage we are not really sure of– no longer exist. Businesses must become more robust, in terms of digital technologies as well as HR and operational management, because the insurance sector is aware of the growing importance of this risk. We must work upstream, because insurance can only be one element of a much larger set of solutions, including risk identification and the organisation of our response. The analysis of possible financial consequences is also fundamental. Some people once believed that a cyber attack would affect their activities for between two and three weeks, but in reality, this period is much longer. Our value proposals will help private businesses to be better prepared.

How does a cyber crisis affect corporate value?

Guy-Philippe Goldstein

Hugo Ronsin
Guy-Philippe Goldstein, what have you learned from your work on the impacts of a cyber crisis on company value?

"The risk of corporate defaulting increased on average by 50% three months after a significant cyber incident."

GUY-PHILIPPE GOLDSTEIN

This question occurs in a very difficult context: the number of attacks has increased 4-fold, ransomware attacks on large corporations have been multiplied by 2.5 according to ANSSI, and the number of attacks on hospitals worldwide has been multiplied by 5, according to PwC. However, even before the Covid crisis, many corporate decision-makers had become aware that cyber risk was now one of the main threats to their businesses, as indicated by the Global Risks Report published by the Davos World Economic Forum and the Bank of England surveys conducted among the top managers of the City of London

The study that we conducted at the end of the 2010s for PWC showed that in two-thirds of cases, for publically-listed companies, share priced dropped by an average 9% in the 21 days following an attack. In 40% of cases, the company turned out not to be resilient and suffered a 20% drop in price after one year; in 23% of cases, the so-called resilient companies, a rebound could be observed, leading companies 12 months later to a stock price of 6% above initial levels before the incident.

For Bessé, we focussed on small, medium and intermediate sized businesses, which represent the foundations of our national economic fabric, and asked ourselves whether the impacts of a cyber crisis would be more or less severe than those suffered by publically-listed companies. Since there is no public data available, we asked data providers for certain
indicators, such as the number of days of late payment or the probability of a company implementing collective insolvency proceedings in the context of a liquidation or a legal redress. Considering a selected panel of 30 companies
(15 international and 15 French), the analysis shows that the risk of corporate defaulting increases on average by 50% three months after a significant cyber-incident. Focusing on the panel of French companies, results show that the impact occurs more quickly (the peak of the crisis being reached in the 2nd month, compared with the 3rd month for international businesses) and that the payment term increases by 50% after the 4th month. Compared with equivalent companies (same size and sector), the

"Cyber technologies imply new industrial quality standards that businesses will be able to use as sales arguments."

GUY-PHILIPPE GOLDSTEIN

default score is much higher for companies suffering a cyber incident. Although these panels are limited in size, it is clear that the directional effects observed are significant. Note that passing the threshold of 1% probability of defaulting (with scores that can reach 1.6 or 1.7% after 6 months) has a strong impact in reducing the total asset value of these companies suffering a cyber attack: by around 8-10%. This is similar to the stock market value evolutions of publically-listed companies.

The consequences of an attack range from significant economic hardships, the most frequent scenario, to bankruptcy (the case of a debt collection company or a B2B2C SME) . In some cases, an incident can also result in demonstrating the company's rebound capacity to both customers and employees. Resilience is based on the following assets:

- Agility and openness in the response.
- Impact absorption capacity.
- Preparation for the impact.

Ultimately, without resilience, the company will suffer from the deterioration of its customers' perception of its brand image and damage to its industrial capacity. Cyber technologies imply new industrial quality standards that businesses will be able to use as sales arguments.

Just how aware are company directors?

Jean-Philippe Pagès

"For us, the cyber risk is currently the topic on which most of our projects with company directors are focussed"

JEAN-PHILIPPE PAGÈS

Hugo Ronsin
Jean-Philippe Pagès, are company directors aware of the potential impacts of a cyber crisis?

Hello everyone. Thank you for your question. The indicator for company director awareness of this risk is indeed essential. It is the foundation for all action. We have been tracking this indicator since 2016 and, when our first study was published in 2018, the level of perception was very low. Today, the strategic nature of this risk has progressed significantly, and no directors are ignorant of the threat. There are several reasons for this evolution:

- The sharp rise in the number of incidents.
- Communication in the media by victims, who warn that all businesses could be affected.
- The health crisis, since the massive use of digital technologies has revealed a number of security breaches for companies.

However, many directors realise that they have not analysed their exposure to this risk in detail, that they have not accurately evaluated their level of cyber security maturity, and, a decisive factor, they have not yet quantified the financial consequences of a cyber attack on their business. However, company managers must evaluate risks, particularly those that may cause losses representing millions of euros for every day of business lost due to information system shut-down. Having a figure enables the director to calibrate his/her actions, to determine a budget and to measure the return on investment.

Due to the systemic and evolutive nature of the risk, the variety of consequences that it may have on the company (hardware, brand image, customer confidence, market share), the analysis is much more complex than that generally carried out for more "traditional" risks. For us, the cyber risk is currently the topic on which most of our projects with company directors are focussed.

HUGO RONSIN
What actually is cyber resilience?

JEAN-PHILIPPE PAGÈS
In 2018, we called for company resilience to be reinforced, because there is no longer any question as to whether or not a company will be affected by a cyber attack: we must assume that such attacks are a certainty. All businesses must realise that they will inevitably be attacked one day: 100%

of hack attempts implemented by specialists are successful. Managing a risk therefore implies management that differs somewhat from the usual process (based on risk mapping with occurrence and cost probabilities), and this is where the principle of resilience comes in. Resilience is based on anticipation of the crisis and frequent preparation, with regular crisis exercises involving all the parties concerned. Such exercises enabled one of our customers, director of an intermediate-size business, to realise that he had not arranged for the expert intervention that would be necessary to restart his information systems after an attack. Let's not forget that if lots of companies were affected at the same time nationwide, competition for qualified experts would be ferocious and the rapid recovery of network operation would probably be compromised. Once the company has quantified the risk and prepared for it, it will be able to bounce back and return to a nominal level of activity, ensuring minimal levels for its essential and vital functions. Cyber resilience will therefore become an obvious competitive advantage.

HUGO RONSIN
What value can cyber insurance provide to a business?

JEAN-PHILIPPE PAGÈS
Insurance will only have any value if the company can manage its cyber risk and prepare to face the crisis. Insurance is just one link in the cyber security value chain of the business, existing to deal with the residual risk once all the defensive measures have been overcome by the attack. It provides compensation for the prejudice suffered, mostly financial losses and consequences in terms of data violation, and covers the costs of expert interventions.

This is a new and growing market: insurers in France cashed around €250 million in premiums (€105 million in 2019), i.e. 1% of the total volume paid by businesses in France, and 5% worldwide. Insurers are aware of this threat and have thus become more cautious. They are professionalising their analyses and raising their requirements in terms of prevention. Insurance is therefore reserved for companies able to prove a sufficient level of cyber security maturity and the existence of a robust cyber resilience plan. We never present a customer's cyber risk to the insurance market without first helping the customer to analyse and evaluate the risk and helping them to build an extremely solid dossier. Without these elements, the insurance market is already unable to propose effective solutions to counter this risk. In the future, this means that access to the insurance market will be a very eloquent competitive advantage for businesses.

Debates

"Cyber security must become an element of company culture, focussing mainly on the human factors, because the crisis is often triggered by an inappropriate click by an employee."

JEAN-PHILIPPE PAGÈS

Hugo RONSIN
Guy-Philippe Goldstein, have you identified any good practices and solutions that could help to build the cyber resilience of companies, on the European scale and beyond?

Guy-Philippe GOLDSTEIN
Resilience comprises not just the preparation but also the response to the crisis, during which the company can show its customers and employees that lessons have been learned and a new standard has been reached.

One industrial group, based in Scandinavia with a subsidiary in France, that was particularly affected has presented its good practices. The main ones are as follows:

- During the crisis, communicate as often and with as much transparency as possible with all partners; ensure specialised communication and provide initial estimates of probable financial impact; communicate with employees, via a YouTube channel, for example, to enable them to share their own difficulties.
- Make careful backups because this could mean not having to pay out a ransom.
- Carry out a crisis exercise at least once a year at top management level, as recommended by the Bank of Israel.

Jean-Philippe PAGÈS
All our studies have shown that the most cyber resilient companies are those that have built a transversal risk governing system involving all stakeholders: IT director, IT security manager, HR director, operational functions, etc. Cyber security must become an element of company culture, focussing mainly on the human factors, because the crisis is often triggered by an inappropriate click by an employee. When managing the crisis, if the company's employees and other stakeholders are prepared and ready to fight the crisis, they will also be ready to help the company to bounce back.

Philippe de BRISOULT
What about cyber security in the public sector?

Guy-Philippe GOLDSTEIN
The French authorities are efficient in fighting IT attacks, but when it comes to protecting essential service operators and national/regional authorities, the level of protection is somewhere between moderate and poor. Risk management is an issue for the public sector and I am not sure that we have the tools to envisage this risk. The attacks against hospitals and town halls have shown that whole segments of the country are inadequately protected. This may be due to a lack of awareness.

Hugo RONSIN
Pierre asks: "Should we not be thinking of insurance solutions that combine the private and public sectors?"

"We have created an ecosystem of service providers available to supply our customers with the technical solutions they need."

JEAN-PHILIPPE PAGES

Jean-Philippe PAGÈS
That is one idea. There are mixed private/public insurance solutions, notably for natural disasters and terrorism risks. They will probably come about, but regardless of the options chosen, it is probable that there will be no sustainable insurance system unless we achieve a sufficient level of maturity to ensure proper operation of cyber security. We believe that it is necessary to call for efforts to be made for the resources required to develop awareness and raise our cyber security maturities levels as high as we can.

Pierrik CHAIGNAUD, Business Development Sales Manager, Anozrway
Cyber security must be part of the DNA and culture of all businesses. As insurers, do you recommend good practices to your customers?

Jean-Philippe PAGÈS
Indeed we do, because we cannot limit our value offer to the residual insurance link in the cyber security value chain. The other links of the chain are essential to the implementation of an insurance contract. We have created an ecosystem of service providers available to supply our customers with the technical solutions they need. Our partnership with Almond for cyber security maturity scoring may raise the director's awareness.

Pierrik CHAIGNAUD
Take a look at what Anozrway proposes, notably in terms of human digital footprints. This service makes companies aware of what potential attackers would see in terms of human cover (known emails, passwords that may have leaked, capacity to be targeted by identity theft, etc.).

Marc WATIN-AUGOUARD, founder of FIC
The topic of resilience is fascinating because it forces us to view cyber security as a collective problem. It is essential that the company's personnel and management share a cyber culture that is neither too optimistic nor too pessimistic. Everyone has their own responsibilities and resilience will depend on the accumulation of individual actions that will enable the company to resist.

Furthermore, we must ensure that cyber security reaches the highest levels of company management, as well as reaching down to the very first person who enters the premises in the morning. The transversal organisation and the response capacity based on clearly-defined structure with major functions, comparable to a military headquarters, is another decisive element that must be considered upstream, before a crisis occurs.

Dialogue between the insurer and the company is also essential. The company prepares for cyber resilience, which is reassuring for insurers, because the cyber risk is becoming increasingly difficult to insure. On the subject of regional authorities, it is clear that the state is certainly not doing enough, in spite of the effort put in. This is why I created the national institute for regional cyber resilience: to bring all public stakeholders together on the same level in these matters.

Hugo RONSIN
Grégoire Lundi, how does ANSSI view the contribution of the insurance sector to cyber resilience?

"We must develop a level of cyber quality that proves that our companies will potentially be less attacked than those in other countries. This will reduce the costs and boost France's image."

GUY-PHILIPPE GOLDSTEIN

Grégoire LUNDI, sector coordinator of ANSSI

I would like to emphasise the benefits of carrying out cyber crisis exercises. Companies can also consult the ANSSI guides.

Jean-Philippe PAGÈS

We always recommend that our customers visit the ANSSI website and download the documentation available, notably the IT hygiene guide, the guide to defining the structure of cyber risk management and the crisis exercise guide. We regularly commend ANSSI's actions in this area.

Guy-Philippe GOLDSTEIN

I can also confirm that the crisis exercise is fundamental, and that preparation should concern all levels of the company, because 90% of incidents are caused by human error. It is obviously better to prepare for crisis management before the crisis actually occurs. Senior management teams and boards of directors should also be included in this policy. It is important that board members are aware of the actual costs of a possible attack.

I would also like to bring your attention to the non-financial reporting of European companies. We should consider including the cyber risk in these reports so that the industrial fabric as a whole understands the costs of a possible attack.

Philippe METTOUX, Director of legal affairs and compliance, SNCF

We have taken steps to cover the cyber risk and have held internal discussions with the company's governing board. Insurance cover of the cyber risk would obviously be unable to pay for the damage caused by a possible attack. However, as for the fire risk, our insurer offers an outsider's view, making suggestions as to where we should focus our efforts.

Jean-Philippe PAGÈS

No sensitive industry can find fire insurance unless it can prove effective prevention measures. This model for the future will enable the cyber insurance market to maintain an offer and to be cyber resilient.

David GUYENNE, President of the Chamber of Commerce and Industry of New Caledonia

Is there a premium for small French businesses? Can we quantify the advantage of being part of France?

Guy-Philippe GOLDSTEIN

There is a vast ransomware campaign currently in the West and ANSSI has suggested that the number of attacks may increase by 255% in France. However, in Israel, which has built a very strong ecosystem of cyber security companies, the number of attacks identified by INCD, Israel's equivalent of ANSSI, increased by just 50% in 2020. We must develop a level of cyber quality that proves that our companies will potentially be less attacked than those in other countries. This will reduce the costs and boost France's image

Conclusion

Jean-Philippe Pagès

I would like to conclude with a reference to the words of General Marc Watin-Augouard: cyber security can only be a collective matter. It is essential that we continue to hammer home this message and contribute to a public-private dialogue that will be essential to our success and the success of our businesses, regardless of their sector of activity and size.

Let us continue to work to raise awareness of the threat and the fundamental elements thereof:

- Risk valuation, because no serious actions can be implemented without figures.
- The company's cyber security maturity: standards for cyber security will one day be established, conditioning access to certain resources, including insurance.

I would like to thank you all for participating in this valuable debate, and I hope to see you all again soon to resume our discussions and continue our efforts in favour of this essential collective cyber security effort.

Hugo RONSIN
Thank you.