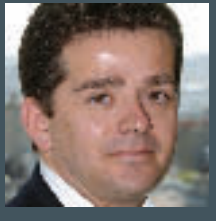
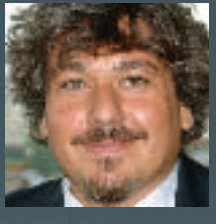
INTERNATIONAL BUSINESS AND PROFESSIONAL MAGAZINE OF THE YEAR

StrategicRISK





# EURO FORUM CYBER RISKS PARIS

IN ASSOCIATION WITH

SOME SAY A SINGLE TECHNOLOGY FAILURE COULD STOP PRODUCTION.

SOME SAY FAILURE TO ADAPT COULD CLOSE THE BUSINESS.

WE SAY POWER ON.

We don't back down from risk, we embrace it. We insure network risk.
Introducing ACE Dataguard™ network risk insurance.
For more information visit www.aceeuropeangroup.com

ace european group

INSURING PROGRESS℠

# Introduction

# The Key Cyber Risks

Far from diminishing in importance, cyber risks continue to rise up the risk manager's list of priorities, as companies become ever more dependent on potentially vulnerable networks and are faced with new threats arising from new working practices. In the first of our Euro Forum sessions, participants discussed the results of a research study conducted by StrategicRISK in association with ACE, which looked at the key cyber risks faced by organisations across Europe.

Seven topics arising from the research were identified by StrategicRISK as offering fruitful ground for discussion. Among them were: improving IT processes and ensuring regulatory compliance, retaining control over security of information, and protecting against external and internal security threats.

Some of the key points to emerge from the debate were the vital necessity of ensuring good communication between risk managers and IT departments, the difficulties of implementing a security-conscious culture across an organisation, and the fact that vulnerability to data loss or theft can involve not simply financial loss, but maybe a potential death blow to an organisation's reputation.

**Andrew Leslie**
Deputy Editor
StrategicRISK

## Participants

**Michel Yarhi**
**Group Head of Insurance, Société Général and President, AMRAE, chaired the discussion**

**Andy Bulgin**
**Director of Risk Management, Coca-Cola HBC sa**

**Gilbert Flepp**
**Technical Lines Manager Continental Europe, ACE European Group Ltd**

**Daniël Jacobs**
**Underwriter, Technical Lines, Property & Casualty Division, ACE European Group Ltd**

**Martin Lesser**
**IT Security Adviser, Bettercom**

**Pascal Lointier**
**President, CLUSIF**

**Jean-Michel Paris**
**Corporate Risk Manager, Bureau Veritas**

**Patrick Pouillot**
**IT Underwriting Manager for Continental Europe, ACE European Group Ltd**

**Fabrizio Sechi**
**Business Security Planning Manager, Fastweb**

**Olivier Sorba**
**Director of Risk Management, Lagardère**

**Patrick Smith**
**European Director, Claim & Risk Management, Hertz Europe Ltd**

**Michael Rossi**
**President, Insurance Law Group**

# Executive Summary

## IT Managers and Info Security Officers commonly bear responsibility for IT security


### Who has DIRECT responsibility for IT security?

| | | | | | |
|---|---|---|---|---|---|
| IT Manager/ Director | 59% | Chief Information Officer | 4% | CFO | 4% |
| Information Security Officer | 33% | Chief Security Officer | 16% | Head, Strategic Resources | 2% |
| Risk Manager/ Director | 16% | IT Security/ IT Risk Manager | 10% | Other | 12% |

Note: percentages do not total 100% as respondents could give more than one answer

During late July and August of 2006, Strategic RISK's research team conducted structured interviews with 50 individuals concerned with IT and/ or risk management in 48 companies and public sector organisations in Europe. The aim was to understand organisations' views of the external and internal IT-related threats they face and to discover the solidity of their defences against these threats.

### What did we learn?

By no means have all companies – even the largest - got to grips with their IT risks. Sixteen per cent, including several multinationals, believe their organisations have only partly identified the IT-related threats they face. But a lot of effort is going into this task. Thanks to rapid changes in technology – and, to some extent, mergers and acquisition – risk mapping is widely viewed as a continuous process. While IT and Risk Managers do most of the work of identifying IT-related risks there is considerable input from other people within organisations.

### Risk Perception and Reality

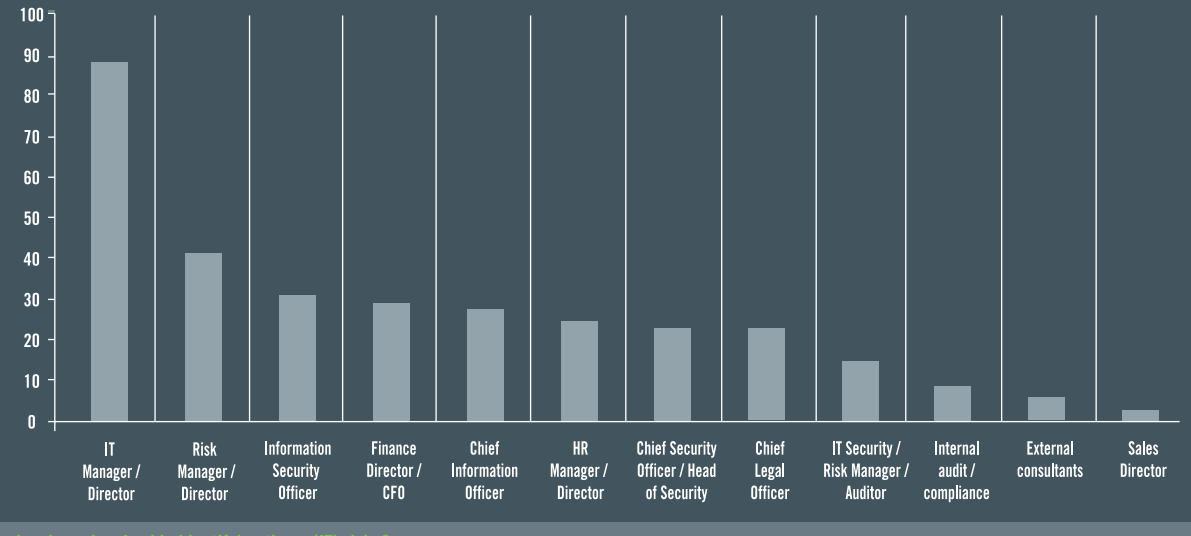
What are the real threats? Most companies see viruses as the main external IT risk, with the risk of data theft or misuse a close second. Other key external threats are public disclosure of private information, and hackers. Extortion against data or systems is the area of least concern. But IT risks arising from physical disasters such as fire, flood, burglary, hardware failure and mainframe outages are viewed as real dangers.

As for internal IT threats, human error tops the table, with employee theft or misuse of data a very close second. The risk of a departing employee taking information and misusing it is a particularly widespread concern.

Companies are particularly vulnerable in some areas. Most prevention or mitigation of external risks centres around viruses, hackers and external electrical outages. Less emphasis is placed on denial of service attacks, defamation or copyright infringement issues, and disclosure of private information. Defences for extortion against data or systems, other malicious attacks and data theft or misuse appear to be even weaker. But the most vulnerable areas for most organisations are the non-electronic theft of passwords, third party fraud and – above all – the failure of IT partners or suppliers to manage their own risks. Some organisations have no controls at all in these areas.

As regards internal risks, most businesses focus on controlling the effects of an internal electrical outage and preventing employee fraud. But fewer believe they have full controls in place for

## IT and Risk Managers do most of the work of identifying IT-related risks




### Who has been involved in identifying these (IT) risks?

| | | | | | |
|---|---|---|---|---|---|
| IT Manager/ Director | 88% | Chief Information Officer | 27% | IT Security/ Risk Manager/ Auditor | 14% |
| Risk Manager/ Director | 41% | HR Manager/ Director | 24% | Internal audit/ compliance | 8% |
| Information Security Officer | 31% | Chief Security Officer/ Head of Security | 22% | External consultants | 6% |
| Finance Director/ CFO | 29% | Chief Legal Officer | 22% | Sales Director | 2% |

Note: percentages do not add up to 100 as respondents could give multiple answers.

data processing errors, employee malicious attacks, theft or misuse of data, loss of or damage to physical equipment and human error.

Organisations have a variety of strategies and tactics for limiting the impact of individual dishonesty, carelessness, incompetence or malice. But those in organisations with particularly serious security concerns tend to have robust vetting procedures – including criminal records checks – plus stringent training and monitoring systems.

In practice – it emerged – the most common cause of actual disruption to IT systems in the past 12 months had been human error. External electrical outage had been the next most common cause of disruption.

**Remote Access, Fraud and Insurance**

Most companies allow certain staff to access their servers from outside the company offices. But remote access is viewed as requiring tight security. Most larger organisations are already enforcing that security. But some smaller, or more old-fashioned businesses look very vulnerable to unauthorised remote access. Remote access is often not limited to senior management, but also includes IT staff, middle management and front-line staff logging in from the field.

Computer fraud losses remain a problem. One respondent in seven stated that they had experienced a material case of computer fraud in the past 12 months. Three of the cases mentioned each involved less than 500,000, but the other four each involved losses of between 1 million and 5 million.

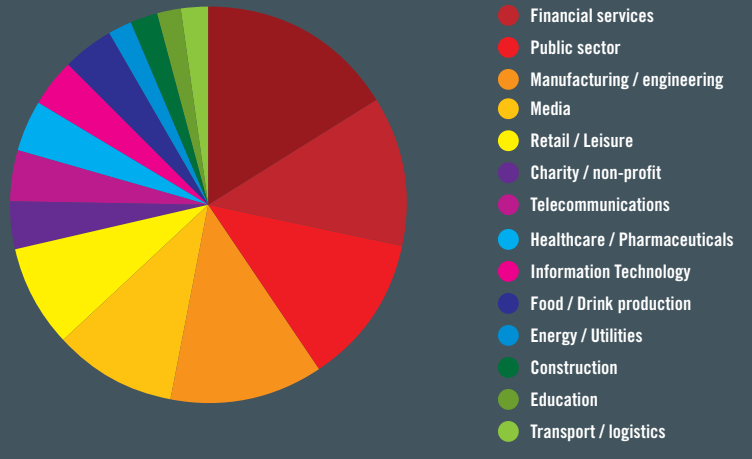
On insurance, it is relatively rare for a risk to be covered by a distinct, IT-specific insurance policy. Companies tend to look to their general commercial material damage and business interruption policies to include some cover for IT-related risks. Several respondents expressed a wish for more clarity, information and advice on this subject.

Overall, only a quarter of companies rated their IT risk management and business continuity planning as 'fully effective'. Most of the rest rated them 'fairly effective'. But six per cent considered their IT risk management to be 'fairly ineffective'. – and ten per cent viewed their IT business continuity planning as 'fairly ineffective'.

In many companies, IT risk management and business continuity planning are hot issues. Many interviewees – several of them relatively new appointees – were conscious of just how much work needed to be done throughout their organisations to catch up to satisfactory standards of protection.

# Respondent Profile

## Respondents covered a wide range of sectors

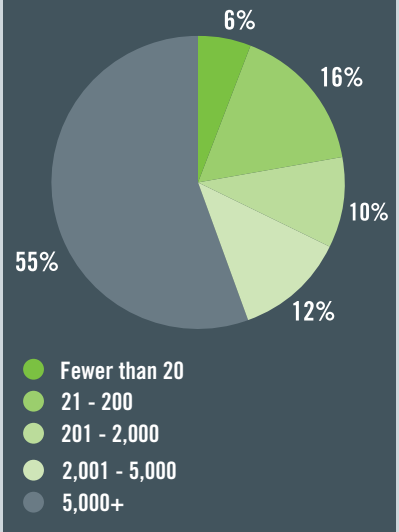



### Respondents by Business Sector

| | | | |
|---|---|---|---|
| Professional/ business services | 16% | Healthcare/ pharmaceuticals | 4% |
| Financial services | 12% | Transport/ logistics | 4% |
| Manufacturing/ engineering | 12% | Information Technology | 4% |
| Media | 12% | Food/ drink production | 2% |
| Public sector | 10% | Energy/ utilities | 2% |
| Retail/ leisure | 8% | Construction | 2% |
| Charity/ non-profit | 4% | Education | 2% |
| Telecommunications | 4% | Total | 98% |

Note: owing to rounding errors, percentage does not add up to 100

## Most respondent organisations employed 5,000+ people or more




### Respondents' numbers of employees

| | | | |
|---|---|---|---|
| Fewer than 20 | 6% | 21 - 200 | 16% |
| 201 - 2,000 | 10% | 2,001 - 5,000 | 12% |
| 5,000+ | 55% | Total | 99% |

Note: owing to rounding errors, percentage does not add up to 100

**Business Sectors**

The largest group of respondents – 16 per cent – described their organisation's business as being professional or business services. Financial services, manufacturing and engineering and the media each accounted for 12 per cent of responses, with the public sector accounting for a further 10 per cent and retailing and leisure eight per cent. The remainder of respondents were spread across telecoms, transport, pharmaceuticals, IT, food production, energy, construction, education and the charitable sector.

**Respondent Organisations' Size and Turnover**

The numbers employed by respondent organisations range from less than 100 to tens of thousands. The majority employed at least 5,000 people.

In terms of turnover, the largest group of respondents – 33 per cent – was in the 50 million to 1 billion band, but 46 per cent had a turnover in excess of 1 billion and 22 per cent exceeded 5 billion in turnover. A few companies were involved in financial or payment services, security, credit information or digital content and therefore enforced extremely high security standards, employing scores or even hundreds of staff in their IT security function. But for most, IT security was more an adjunct to routine business.

**Do you sell goods or services through a website trading platform?**

We asked interviewees whether they sold goods or services through a website trading platform. Fifty-two per cent said they did. Eliminating the five public sector bodies raised this percentage, but only to 53 per cent, as – perhaps surprisingly – two of these bodies claimed to sell goods or services in this way.

**Do you sell goods or services through a website trading platform?**

| | |
|---|---|
| Yes | 52% |
| No | 48% |
| Total | 100% |

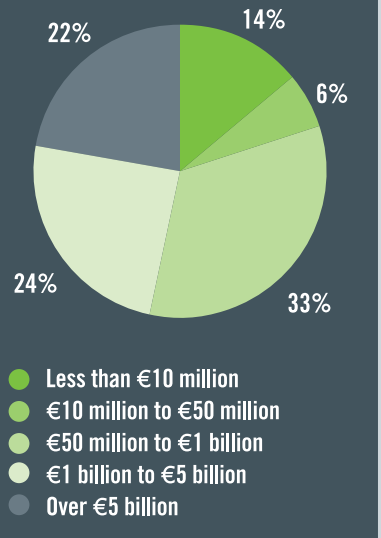
**If yes, is this business to business, business to retail consumer, or both?**

Of the 25 respondent organisations that did sell goods or services through a website trading platform, five did so only to other businesses, while five did so only to consumers. The remaining 15 - 60 per cent – sold to both.

**Does your website have facilities for receiving personal information from visitors, such as credit card or address details?**

Although only 52 per cent of respondent organisations sold goods or services through a website trading platform, 59 per cent had facilities for receiving personal

## Nearly half exceeded €1 billion in turnover

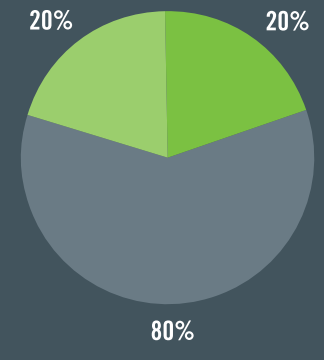



**Respondent organisations by turnover**

| | |
|---|---|
| Less than €10 million | 14% |
| €10 million to €50 million | 6% |
| €50 million to €1 billion | 33% |
| €1 billion to €5 billion | 24% |
| Over €5 billion | 22% |
| Total | 99% |

*Note*: Owing to rounding errors, percentage does not add up to 100

## Six of every ten web trading platforms were both B2B and B2C




**Is this business to business, business to retail consumer, or both?**

| | |
|---|---|
| Business to business | 20% |
| Business to retail consumer | 20% |
| Both | 60% |
| Total | 100% |

information from visitors, such as credit card or address details, on their websites. In some cases, this was as elementary as a sign-up process for newsletters or the facility to upload CVs or register for a course or conference.

**Does your website have facilities for receiving personal information from visitors, such as credit card or address details?**

| | |
|---|---|
| Yes | 59% |
| No | 41% |
| Total | 100% |

**Does your company or organisation have an intranet and/ or an extranet and do they use company laptops for mobile working?**

Ninety-four per cent of the respondent companies interviewed said they had an intranet. Only six per cent – three companies - said they did not. All three were small companies with fewer than 200 employees; two of them employed fewer than 20.

As for extranets, two thirds of respondent organisations used them. Those that did not use extranets included 80 per cent of public sector bodies – but only 13 per cent of the organisations with over 1 billion in turnover.

Laptops and other portable electronic devices are now practically ubiquitous in business - and as we shall see, they raise distinct security issues. At one respondent's business, a third of the workforce normally worked remotely from customers' premises. "We have 60 offices in 23 countries and employees can go to any of them, plug in and go." Of all the respondent organisations, only one said that no staff used company laptops for mobile working.

If you would like to receive an electronic copy of the full cyber risks research report please contact Patrick Pouillot, IT Underwriting Manager for Continental Europe, ACE European Group Ltd on **Tel: + 33 01 55 91 45 45 or** email **patrick.pouillot@ace-ina.com**

# Cyber Risks Roundtable

**MICHEL YARHI:** I fear we have less than two hours to deal with seven different topics suggested by Strategic Risk. That's not a very long time for each item; about quarter of an hour each. If you want to, we can take them one by one and try to give some answers from your experiences in the field, and discuss how to manage the different kinds of risks. The first topic is how to improve IT processes and ensure regulatory compliance. Who has experience of that issue and wants to begin?

**PATRICK SMITH:** Shall I talk about Hertz? I'll start by saying I'm fairly new to Hertz, and new to a global organisation. So, part of my preparation for coming here was trying to find out who might be responsible for this kind of area, accepting some responsibility myself, and I was told it was probably somebody in Oklahoma City, who spent all their time dedicated to the control of data, but who's on vacation at the moment. So my preparation was difficult. I think my overall observation is that we have rigorous IT rules. We have password protection that runs out almost by the hour; we have screens that, if you stand up from your desk, they lock down, and when I work from home, I have a 50% success rate of being able to get in, not because I'm doing something wrong, but because there is an inbuilt procedure which says 'Let's not make it too easy for them'. There's a helpdesk number and I'm straight through to Oklahoma City, and

## ONE CAN BECOME HAMSTRUNG BY PROCEDURE

**PATRICK SMITH**

they apologise, but they must validate that it's me. It's like phoning my bank; they want my postcode, my zip code, my height, my date of birth, and then they give me my password back. So we have a very rigorous approach from an IT perspective, supported…

**MICHEL YARHI:** Excuse me, sorry, are there specific rules at your company, which are official and that everybody has to apply ?

**PATRICK SMITH:** I will receive on a daily basis from our procedures department three rules a day, generally re-written ones rather than new rules. And it's very difficult to know what's relevant and what's not relevant. What binds it all together is SOX compliance. It brings in an environment where people check first, and I've come from smaller organisations where flying by the seat of one's pants is more normal. There are risks involved in doing that, but there's a caution with the checking first too, because you can't remember 3,000 procedures all at one time. But it's a way of working. I think the only risk I see is that, while on the face of it we have a very solid approach to external risks, one can become hamstrung by procedure, and there are occasions when you wonder at what time in the day you're going to be able to start to do some work.

**MICHEL YARHI:** What is other people's experience? I suppose that in each

## THERE IS A LARGE ISSUE OVER HOW YOU HANDLE PERSONAL DATA

**OLIVIER SORBA**

company you have internal rules about IT, so what's the level of constraint imposed by the rules? Are they very strong? light? how do you live with them?

**ANDY BULGIN:** I think it very much depends on the type of organisation that you have, in the sense of flexibility and autonomy of operating units. If you look at Coca Cola HBC, we have a central framework, but we have a degree of autonomy operating at a country level. So the question when you apply that in an IT context is: do you make it an absolute rule that people have to do certain things, buy certain systems, work in certain ways, even if that might be detrimental to their overall profitability? Or do you have a degree of flexibility in how people are allowed to operate? – which then of course increases the risk of non-compliance or damage to the organisation. I think the balance is very hard, and, from what we have just heard, if you have to spend an hour a day working on updating yourself on what the current procedures are for you to operate within the business, then I would consider that to be a major impediment. If we consider that IT is supposed to be in the nature of a release mechanism to make all of us perform better, then there is a little bit of conflict there between the two concepts.

**JEAN-MICHEL PARIS:** Maybe in terms of pure IT processes, I could share some of my experience within Bureau Veritas. What we decided to do was to split the IT and IS teams into two, so what we've got on the one hand is a corporate team looking only at infrastructure and operations: that's really the pure IT hardware, the links, the connections, the hubs, the shared service centres. And on the other hand we have a second team that looks at the applications themselves. The reporting lines are interesting here, because ultimately they both report to the same member of the management board, but through different channels. That way, it's designed to keep a check and balance on the combination of the pure IT aspects and the applications. And the overall policy that we have is a combination of what these two departments produce. So that's in terms of pure IT processes; it enables us to have a level of comfort from the fact that one team is actually under the eye of the other team at all times.

**OLIVIER SORBA:** The question also involves regulatory compliance, because there is a large issue over how you handle personal data. The first question is, do we know exactly what the law is and what we can do and cannot do? And the problem with a global group is that you end up with different regulations in different countries and then the question becomes who is responsible for checking? Do even people know that there are laws on the subject? I'm only talking about the legal risk, and even that's a topic as itself.

**PATRICK SMITH:** The approach at Hertz has been to take the most serious approach to data protection and apply that globally in every territory.

**OLIVIER SORBA:** Sometimes you don't even have the right to hold data. Even if you do things absolutely properly and with absolutely no glitch in your system, sometimes you do things that are not allowed, perhaps because you joined two files that should not have been joined. And it's a challenge to even know what the laws are about things like that.

**MICHEL YARHI:** And to know the law in each country, because if it is a world-wide company they have to adapt themselves to the legal systems of each country. It's not easy. Is there anything else about regulatory compliance?

**MARTIN LESSER:** I would like to know whether, for example, budgets for IT security are being raised for this year or next year, or are you keeping it the same as one or two years ago?

**PATRICK SMITH:** Good question. I don't

know the answer. There is a lot of IT development work and I would suspect that as systems become more complex, there's a line of cost that is probably more significant than it was 10 years ago. I can remember that, 20 years ago, cyber risk didn't really appear on the IT spectrum. We are putting in place a new claims management system right now, which is internet-enabled, so there's lots of client benefits to it, but there's inherent risk too, unless one has that string of security. And not only one that complies with Hertz' requirements, but we have external clients, and it needs to meet their requirements too.

**MARTIN LESSER:** I asked this because, in Germany, we have a federal office for information security, and they did several pieces of research last year, involving many companies One result was that every company saw a growing risk in IT security, but only 39% of those companies had raised their budgets for IT security. 40% were keeping it the same as the last year, and the rest actually had shrinking budgets. Personally, I see an increasing number of risks, especially when you think about the internet. We are seeing a totally new quality in attacks. Four or five years ago, there were many spotty guys who tried to hack, and it was fun, but now there are really criminal organisations from Romania, from Brazil, from China, especially Korea, who try to attack systems, and I personally see the risks appearing not just for big companies but for the smaller ones too.

**MICHEL YARHI:** And of course it depends on the activity of each company. Speaking as a person working for a bank, you can imagine that banks are very concerned by IT security in general, software, and the internet of course, because most customers no longer go to branches; they do everything on line. And if it is not secure, we are dead. So today the most important question is: at what level in your different companies does the sensitivity to the risk, and how to manage and limit it, lie? Is it the first concern of your chairman? Or is it something less important? I can say that for us, as a bank, it is first, at the top, after the financial risks, but I suppose that to all of you it is something important? You have to say yes, because there are some insurers around the table. Okay so we see the first issue…

**GILBERT FLEPP:** There's just one question I would like to raise about regulatory compliance and that is whether the process of compliance has changed the perception of the risk, or if it has allowed your organisation to identify misbehaviour or areas of risk exposure which were not properly assessed before?

**MICHEL YARHI:** Does anybody have an answer?

**OLIVIER SORBA:** We are not SOX-registered, which is why I am answering. True, there are other regulations that are less stringent, but that kind of risk was starting well before many of them, as were the efforts to deal with it, but now we are being forced to deal with it in a very organised and structured way.

## THE STAKES ARE RISING

### JEAN-MICHEL PARIS

**MICHEL YARHI:** In fact, we don't need SOX to work in that way. Just before coming here I was preparing another conference about internal control. That's the day to day problem: internal controls have to be set up in all companies, not because of SOX or anything else like that, but because it's a problem of life or death for a company. If you don't monitor your risk, you can't live, because a single virus can kill you.

**JEAN-MICHEL PARIS:** I think that's becoming even more true now, because more aspects of our daily work are dependent on specific applications. That wasn't the case before. Before, there were just your standard applications like Word or Excel or whatever, which didn't really need any specific developments for specific processes or delivery of certain types of services. Now, ERPs are obviously everywhere, so you depend on them for the internal function, and it's the

**NOBODY WHO'S DEVELOPING SOFTWARE TODAY THINKS ABOUT KEEPING IT SMALL AND SIMPLE**
**MARTIN LESSER**

same for other applications, like PeopleSoft for the HR function. So the main internal functions depend on them, and then the delivery of the work, depending on which activity we're in, is also dependent on specific applications. So the stakes are rising. And when you ask how important is it for your organisation, the answer has to be that it's very high, and rising.

**MICHEL YARHI:** Okay, second issue, retaining control over security of information. It's quite an important problem. Who retains control? Pascal, we still want to hear from your association. Do you have some information about your members?

**PASCAL LOINTIER:** Not at the moment, because it's really an internal problem, so I think it's better for people from their own companies to explain what they do. I have some comments about other topics, but not on this one.

**MICHEL YARHI:** Okay so no reaction to this issue?

**MARTIN LESSER:** There is one interesting point in the (Strategic Risk) research, that I read yesterday. Anyone who has answered the questions about their controls as having absolute confidence in them is deluding themselves. I think that's the truth. You will never have full control over IT security, in my opinion, the systems are too complex. It's not possible to get full control.

**MICHEL YARHI:** And sometimes the software is so complicated that we don't use 100% of its capability. You use 50%, even 75%, but never 100. So the problem is the remaining 25%: what are the potential risks linked to the unknown and unused portions of software? And that's a problem.

**MARTIN LESSER:** In software development there's an old philosophy called KISS – keep it small and simple. But nobody who's developing software today thinks about keeping it small and simple. They try to implement more and more features, and every new feature can build in new risks.

**MICHEL YARHI:** And how are controls set up to limit that kind of risk?

**ANDY BULGIN:** I think the whole problem with IT control is that the majority of us don't really understand IT particularly well, because IT professionals speak a different language to the rest of us anyway. So when you're talking about it in a control, or even in a Sarbanes-Oxley context, where the IT team tell you that they have certain controls in place, are the people who are actually the custodians of it qualified to comment whether those controls are adequate or not? If we don't understand how all these systems work, how can we be sure we have adequate control? And control, I think, in all these contexts comes back to the behaviour of individuals within the company. You can't control what you don't understand.

**MICHEL YARHI:** Are there people specialised in IT activities in the different audit departments? Because that's a key point. Is the audit department able to understand what we are delivering and how we deliver it?

**JEAN-MICHEL PARIS:** I think it's typically a challenge for people from the risk management and audit function to go to the IT professionals and say 'Can you demonstrate that what you're saying is true?', and by doing it in a way that demystifies all that IT jargon. And you can either do that internally or commission people from the outside with the specific skills to do it, it doesn't really matter which, but I think the crux is whether you are challenging the people responsible for the IT systems. I would add that this challenge must be continuous, because if it isn't, then it becomes a case of poachers and gamekeepers, and we know who usually runs faster.

**PATRICK SMITH:** This interface between IT and operations is the key challenge, plus the issue of whose responsibility it is. There's a risk in planting the audit function firmly on specialists, because they're not necessarily business specialists, and also, one of the major cyber risks is misuse by employees who aren't in the IT department. Left to specialists, potentially you'd end up being able to transact absolutely nothing, but would be 100% safe, so that would be good news. Unfortunately, you'd run out of money, so that would be bad. So I think the starting point is to ask what you would like the business to be able to deliver through the IT. Start there, rather than with 'Let's have a look at the IT'. But equally, in the right environment, it's sensible to have a specialist at the table. So I think it's about having the right people around the table. If you decide that your internal audit is your policeman, then they need to understand what the commercial realities are, what we are trying to deliver as a business.

**MICHEL YARHI:** Something else about this issue?

**OLIVIER SORBA:** Sure, auditing is important, but I have a feeling that it

takes a lot more. Maybe you need your own IT guy to help you organise the way you look at the others. You need something organised, because my feeling is that when you deal with large organisations, and different countries, it's a matter of the degree of pressure you put on the system. Things are complicated, and you cannot go into each and every detail, but you want to know that someone competent does, and that the general policy is followed, and do you do that by auditing? Anyway, you have to do something organised throughout the organisation. That's my feeling. Audit is part of it, but I think it takes more. For example, an important part of controlling the risk is that the security decisions are consistent throughout the organisation, so you need a policy and you need to talk to people. Obviously in a bank it must be something very stringent, but I think that with a bank you have the power to decide something at the top, to say "okay, the way a client talks to this webpage will be the same everywhere." Sometimes it's different; people have different businesses and different traditions throughout the world and you have to adapt.

**MICHEL YARHI:** Let's move on to the next item: 'Understanding potential exposures and communicating them to management, and employees'.

**PASCAL LOINTIER:** I suspect that everybody will agree with the idea that organisation and human management are key factors for success in IT security. But the trouble is that not many people have much understanding of psychology. If you want to convince someone, or a group of people, to do something, you have to have some knowledge about communication, motivation and behaviour, about how to invite someone to do something, how to convince someone to do something. This is nothing new; this is not magical; this is purely about communication. If you want to communicate with your people you need to know the techniques, but most of the chief information security officers, or network administrators, do not know them or do not think to use them. As a result they will just make some rules, but with no understanding of people's motives and no understanding of whether people will accept these procedures or not. So I think it's very important. We all speak about the human factor, but I never saw CISO or network administrators having human communication training.

**MICHEL YARHI:** And to have a psychological approach?

**PASCAL LOINTIER:** Absolutely. The right words at the right time and so on. It's manipulation, but it's good manipulation.

**DANIËL JACOBS:** It's also a very difficult task. If you take, for example, USB sticks, I get one from a client about every two weeks I think. We love them; you can put your entire client base on a big USB stick and just plug it in. And if I get it every two weeks… Well, at present there is no rule for us about not using them, but there is potential risk, and that's a very difficult task to explain to everybody.

**PASCAL LOINTIER:** But, for instance, if you take budgets, there are tricks you can use. Let's say you want to have something which costs 100 euros, you will say 'Okay, it will cost 150 euros', and then when people object you say 'I've managed to get a deal, and we can get it for only 100 euros' and people are happy because you have reduced the price. I don't say that it will work every time, but it's a good trick. It's the same thing for convincing people to do something: it's better when you make them think about it instead of forcing them to respect rules. But those IT people don't think about using communication roles to have a better understanding and better enforcement of policies.

**ANDY BULGIN:** You can argue that the IT people shouldn't be the ones responsible for communication to the organisation anyway.

**PASCAL LOINTIER:** Not communicating about everything, but about things they are in charge of. In France we have a charter for end users; people have to sign a document saying that they will only go on the internet for professional use and so on. Instead of having this signed by people without giving any explanation, it's better to explain why. You don't have to transform yourself into a communications person, but just do the same thing that you would do in your private life.

**THERE IS POTENTIAL RISK, AND THAT'S A VERY DIFFICULT TASK TO EXPLAIN TO EVERYBODY**
**DANIEL JACOBS**

**ANDY BULGIN:** Sure, I understand that, and I'm not arguing with the psychological route to try and persuade people to do it, because it's a sensible thing to do and it makes sense to them, rather than just making it a hard and fast rule. But the issue is more about IT as part of a general code of business conduct. We don't necessarily get that linkage, because of the mystification around the technology that people don't understand, but if you look at risk management in general, you're trying to force a level of personal responsibility on every employee within the company, and the same should be true of IT. So if you're going to talk about the use of USB sticks for example, if you take it to the extreme,

**EMPLOYEES KNOW THAT DOWNLOADING CAN POSE A HUGE RISK FOR THE COMPANY. BUT THEY STILL DOWNLOAD THINGS**
**PATRICK POUILLOT**

people should be reprimanded when they're seen using them and ultimately it should lead to dismissal, if it's seen as being a major issue within the organisation. It's very, very difficult to control, but if it doesn't have teeth, then no-one will take it seriously.

**PATRICK SMITH:** I suppose the other thing is that there would be a very sensible business reason why you wouldn't use USB sticks, and if that could be articulated, then the IT department, as well as every other, would understand that a business risk has been closed down. In previous jobs I've struggled to find that the IT department necessarily understands what the business is about. If there is a perception that they are poor communicators, does that mean that we stop communicating with them, so they become very isolated from the business? Where the overall risk increases is in our complete reliance on IT systems. And the business challenge is to make sure that no one department becomes polarised.

**JEAN-MICHEL PARIS:** On the topic of communication and IT people, I feel I should defend them a little bit. In my current organisation there is actually a reasonably good degree of communication. There are published KPIs as to up times, down times, all sorts of KPIs, application by application and so on. And it's there for all to see; it's on the intranet; you can just click on it and see it any time of day. I think the challenge is the same as for any support function; it is how much of a business partner are you?

**MICHEL YARHI:** Any reaction to that?

**PATRICK POUILLOT:** Maybe just one word concerning understanding potential exposures. As an insurer, I think we have now standard coverages for viruses, and I think everybody understands what the risks are concerning viruses, and employees know that downloading can pose a huge risk for the company. But they still download things. Understanding potential exposure is not enough. Even where you understand exposure, you can have some behaviour that should not be allowed in a company. But that is the way it works, and that is the reason why there are insurance companies that sell insurance products for IT. So understanding is not maybe the key word. The way we react as a company against people that illicitly download files is important.

**MICHEL YARHI:** If you are speaking about insurance, may I remind you that insurers have set retentions? That means that, as a company, our interest is not to have any problems, and that's the reason why the more we are involved in security, the more everyone is happy, because we are not involved in the risk. So, when you are a big company and the retention is high, your first interest is not to suffer any kind of loss. That's the reason why we have to communicate, and, even if we don't give all the details, each player has to be a part of the global theatre to ensure the company does not suffer any kind of loss.

**FABRIZIO SECHI:** The biggest issue in our experience is the cultural situation. What does this mean? Because we are a telecom company, we have a lot of employees that work in IT and network departments, and these people give a lot of importance to the topics of security, monitoring security, of technical security. Our biggest problem is with the marketing department, and with the customer relations department, because the interest of these departments is not security. It is to sell, or to have the best level of service for our customers, and so the problem of security is not a big topic. Our job today is to increase the culture of security and explain that bad security can make a loss for the company. This is more important than the best anti-virus system or the best firewall. It is a cultural problem, a cultural problem absolutely.

**ANDY BULGIN:** I think that's a very interesting point, because in most risk management issues you can get to the

**OUR JOB TODAY IS TO INCREASE THE CULTURE OF SECURITY AND EXPLAIN THAT BAD SECURITY CAN MAKE A LOSS FOR THE COMPANY**

**FABRIZIO SEECHI**

bottom of root causation of loss, relatively easily… you can narrow it down to a few things. In terms of IT, root causation of loss could be the actions of any one, in our case, of 40,000 employees who have access to IT equipment. But if you ask me what is the biggest issue, would it be the failure of one of our servers? I'd say no, that probably wasn't what we would see as being a major issue. I would say it's loss of confidential information on a PC or on a flash drive in an airport. But training 40,000 people to know what the consequences are and what they can do and can't do is an absolutely enormous project; it's going to cost you millions in a training budget to do it, and a lot of people will baulk and say 'Oh it's not that bad', but it is potentially that bad, and we don't even have the customer focus, the risk of holding very sensitive personal data. We have a very small amount of that, but we do have an awful lot of confidential information that is widely spread across the entire population of a business, and trying to keep your hands on that, I think, is an almost impossible task.

**MICHAEL ROSSI:** And if I can add, as an observer, probably the only lawyer here, who advises companies on these issues from an insurance perspective, the one thing that hasn't even been mentioned is theft of data. It happened to a well-known insurance company in the US whose server was in a room; someone came in through the ceiling, just like out of Mission Impossible – this is no joke - and the whole server was unbolted from the floor, lifted up and taken away. But that's just an example of one of the things that hasn't been discussed: the premises liability and premises security. IT people are more prone to thinking in terms of hacking and things like that, whereas… well who's looking out for the protection of the premises? or theft of the computer laptops and stuff like that? To me, somebody needs to take ownership, and I think it would be someone within the risk management department, like the chief risk officer. We mentioned privacy, and legal liability risk arising from it, but the IT people aren't thinking about that; they're thinking about the system going down and suffering losses, or the data being stolen and having to re-create it. But someone needs to take ownership of all the different ways that this information is at risk, and then delegate and report up. As a lawyer to companies, I just see a spaghetti on the wall approach – perhaps that's crass – but there's no one cohesive strategy for addressing it all. I think it's because people are still struggling with the newness of it.

**OLIVIER SORBA:** It goes back to the global approach and how you need to gather the risk people, wherever they are, and the IT people, to look at networks and their communications from a risk point of view, and you need both the risk specialist and the IT specialist. If you don't have both, you fail. Another point

**THE LEVEL OF INSURANCE THAT THE PROVIDER CAN HAVE IS ALWAYS LESS IMPORTANT THAN THE RISK WE TAKE WHEN WE USE AN EXTERNAL PROVIDER**
**MICHEL YARHI**

is, talking about ownership and things like that, that you always end up asking people to change their personal behaviour and/or spend money. So if you don't have management commitment to the effort, it's not even worth starting. Basically, the IT people and the risk people on their own don't have the power to ask people to change their behaviour and change their culture and so on. So management commitment is very important in order to achieve success.

**MICHEL YARHI:** Anything more on that? Okay next topic. 'Assessing IT providers to ensure compliance with information security policies'.

**PASCAL LOINTIER:** I don't use them personally, but may I comment? I think that most people are too confident in the name, the brand name, of their IT supplier or IT provider, instead of assessing operationally the content of agreements and how they will be enforced. I've heard that some providers or data centres do not enforce the security rules that they say they will provide in your agreement, because it costs money. It is as if you were asking about, let's say, a fire extinguisher, and they will say 'Oh we have it for you', but the day there's a fire there is nothing, and so: 'Okay you can sue me, but you know that a third party trial is very limited compared to the business impact for you', and this is a … I won't say that all of those data centres and ISPs will react like that, but it happens.

**MARTIN LESSER:** Another point is, how can you ensure that your IT providers meet your own policies?

**PASCAL LOINTIER:** You have to check, send in some people from your own diligence to audit their system, or visit by yourself if you have the knowledge, but you have to do it; you can't rely only on the agreement.

**MARTIN LESSER:** Six months ago in Germany we had a bad incident with a provider who provides services for companies who sell things on eBay, and this provider was sacked and data from large companies was stolen and passwords changed and so on. But I don't think any companies checked the infrastructure or especially the software, which turned out to be insecure. But I think it's a really big deal to check every provider you have and the software he uses; you can't do it. You can have a look and you can do some audits and you can talk with the provider, but it's absolutely impossible to have a look at each piece of software the provider uses. So the risk remains.

**ANDY BULGIN:** I think there are two issues. One of them is the technical reliability of the person who you're outsourcing to: will the system fall over? and, if it does, how quickly will you recover it? The second is the trustworthiness of the people that you're outsourcing to and their third party handling of your sensitive data, because that goes back to the point you were making from a legal perspective. I don't know how many companies are actually doing security audits on people that are coming in from a third party perspective. We wouldn't do it from a production perspective, but, arguably, it should be being done always from an IT perspective because of the sensitivity of the information.

**PATRICK SMITH:** To me it's comes down to cost/benefit analysis. There's software there that will do 80% of what I need, and the aim is to acquire the last 20%. So how do I make that happen? The approach that I take, which is often taken within Hertz, is that actually we're not outsourcing IT; we're getting some external software, but we still own that software; we still own the risks; we own the benefits; it's ours, protected by a contract and SLAs and all the rest of it. And the whole procurement and implementation process has been using the strength of IT people as part of a team to ensure that … I think the point is we are not reliant on asking the vendor 'Is it secure?', and they said 'Oh yes it is, ever so secure' 'Oh lovely, thanks'. My view has been to know my own boundaries and try to work out what we don't know and invite my IT friends to come and help. And I think if we talk about culture, the behaviour of moving, in this instance from a self-build to going and buying something configured, has been helped by using the IT experts, for what they're good at, which is to understand the parameters and the risks and the security.

The other point I was going to make, is that part of the reason we are modifying this software, part of the benefit to us, is the ability for my people to work differently, and I think that's one of the emerging risks. When I started work you very rarely left with a piece of paper in your hand at the end of the day, now we encourage people to work from home, and that's really great news. We encourage our clients to come and look at their data, to come and do stuff online, and we do that in our business widely, and we encourage it, because it makes commercial sense. However, we as a business need to keep in step with the

risks that we are creating. And I think one of the benefits in creating a team that's protecting the business is that my friends in IT don't receive StrategicRISK, but they do receive IT Weekly, where they find all the anecdotes of things that have gone wrong., I wouldn't understand them, but they know what they know and I know what I know, and actually if we get together we might make some smart decisions.

**MARTIN LESSER:** There's an issue though for IT managers in big companies, that if the risk manager comes to them and asks 'Do we have any remaining risks?', and they say 'Yes, I have some remaining risks', that their standing goes down because they haven't fixed all the risks. There's a danger, if you as risk manager ask your IT guys 'Do we have risks?', that they will say 'No, we don't have risks', because they want you to think well of them.

**PATRICK SMITH:** Often it's the way you ask the question I suppose. My view as a risk manager is that there isn't a correct answer. There's either risk or there isn't, there's an honest answer to a straightforward question. Now, some level of risk might be acceptable, it might be impossible to be completely risk-free, but a realistic assessment of how big that gap is and then choices to whether you insure or embrace it as part of the financial structures of the business, they're choices you make. I think the team selection and working together and sharing the objectives of the project is the best way to avoid asking leading questions where you're never quite sure whether you've got the right answer. If you were very cautious, you'd never launch, because you'd always have that sense of nervousness.

**MICHEL YARHI:** How do you manage the constraints where you have the problem of money, where buying from your provider is less expensive for your company, but may mean less security and less quality. And are there discussions between the purchasing department and you, or is each one free to do what he wants?

**PATRICK SMITH:** My experience working together with procurement, is don't pay up front. I think you will receive the risk that you create. If you pay your project fee or your licence fee at the point you start tailoring something, then financially you're in it. So we've worked in this project with a way of graduating the payment stages so that there's every incentive for suppliers to meet our needs.

**FABRIZIO SECHI:** We are in a strange situation, as we supply technology and we also buy a lot of IT. We work in partnership with suppliers, and then the supplier knows that our goal is the same his. But I am curious to know your position about third party audit and certification, like BS, because for us it's an expensive asset, but I am not sure that the security experts agree on this point of view. Is it important for you to know that a company that can provide you with technology has a certification?

**MICHEL YARHI:** For us, it's very important when you use external providers to check the quality of their services at each level, because the consequences for the bank are always more important than the consequences for the provider himself, and the level of insurance that the provider can have is always less important than the risk we take when we use an external provider. So we are obliged to check the quality of the service and we use an external provider only when we are sure that they are the top quality.

**ANDY BULGIN:** I think the question is, Michel, is your assessment of quality on the basis of certification? so if you went to Fabrizio's company, would you say, because he has that certification, that would be a reason why you would purchase from them without any further checks? Because, if not, then the value of having that certification is questionable.

**MICHEL YARHI:** Well probably if the certification …. We all know that certification, let's take, for example, ISO, doesn't mean anything. It means that you are able to do such a thing in such a time. But if your standards are very bad…..

**ANDY BULGIN:** But I think that's an interesting point. Does it mean that that's

**ANOTHER THING IS TO MAKE PEOPLE RESPONSIBLE FOR THEIR DATA**
**PASCAL LOINTIER**

the bare minimum that you have to get, and if you didn't have it you wouldn't be considered at all, even though the standard doesn't actually mean anything? Because I think it's then questionable in this environment whether it's worth having these standards.

**MICHEL YARHI:** Anything else? We have to go on, because there are three more topics. 'Creating a security-conscious culture'. We spoke about that a little bit before, but maybe we can add to it.

**MARTIN LESSER:** I would like to bring up a little problem between marketing and IT security. For example, in Germany, the Federal Office for IT Security recommended several years ago that all users should disable Java Script in their browsers. But if a user did that today, most web pages, especially web pages from large companies, wouldn't work any longer. So we have a dilemma between the recommendations for IT

## THERE IS A STRONG NEED FOR BETTER CONVERGENCE

**GILBERT FLEPP**

security and the recommendations from the marketing people. In the past, in my opinion, the marketing people won the race. But in the future, we will probably see the security people win more and more, because the risks are growing.

**MICHEL YARHI:** Any other experiences? How do you manage in Ace, as a company?

**GILBERT FLEPP:** Well I'm just thinking of an interesting case where we bought in from a telecom company, and to show that their service was the best in the country, they wanted to provide all their clients with a CD-ROM that was delivering a lot of additional services. And what happened is that this CD-ROM, about 30,000 of which were printed, happened to be infected by a virus and they had to recall it of course. So it touches two aspects, the one before, and the conflict between marketing and security.

**MICHEL YARHI:** Anything else about this?

**PASCAL LOINTIER:** As far as France is concerned, we would recommend using end user charters, because it's a good way of convincing people, and, if there is a legal issue, you can use that document to prove that you tried to inform people about their rights and their duties regarding the internet. Another thing is to make people responsible for their data, and not have the feeling that there is some specialist somewhere who can magically restore data and passwords.

**ANDY BULGIN:** Do you not think that we suffer a little bit from password fatigue generally? I have a friend who had so many passwords that in the end he had to write them down, which kind of defeats the purpose. But if you're talking about protection of data, we all have so much data, somehow someone's got to be able to keep track of it, and it gets to the point where I think it's almost impossible. So that in itself is quite a risk.

**PATRICK SMITH:** This is the point about culture. The password issue arises from the fact that you don't trust everybody not to release their password, and you're trying to create a culture where you trust people not to release their password. So it's very difficult.

**MARTIN LESSER:** But if you look at the normal daily business, people sit together in an office; something doesn't work, and next thing it is, "please let me go to your computer, or please give me your password" and so on; there's a social atmosphere, so everybody trusts each other, and many people don't see any reason for not giving their passwords at least to a colleague, for example. And it's difficult to prevent that happening.

**DANIËL JACOBS:** But you're not going to give the password of your credit card to your colleague 'Please can you get to the bank and get 50 for me?'; you're not going to do that. It's just the culture.

**MARTIN LESSER:** Yes, it's the culture, but the normal staff member does not think that way. It's a different matter giving his colleague his credit card, from giving him a password which is effective only for his business, for the corporation he works for.

**PATRICK SMITH:** I think it comes down to the way these things are communicated, in that all too often the disadvantage of taking a certain course of action is all that's communicated. Not the advantage, always the disadvantage. And sometimes… 'and here's the penalties'. So you're ruling by fear, rather than a culture that says 'Here's good business practice, and here's why, here's some of the benefits.'

**GILBERT FLEPP:** And to improve this culture, security culture, there is a strong need for better convergence between the many different responsibilities of an organisation, and this is very time consuming and extremely tough.

**MICHEL YARHI:** Concerning the example of your credit card, if I can make a comparison, we can consider that people working for a company are linked by the same wish to do the best for the company. It's the same between a man and woman

when we are married. Sometimes you can give the code of your credit card to your wife, because you consider that you are in the same boat and that you do together what is best for the family. So it's a very touchy subject, but the problem is what kind of confidence you have in the other person. Okay, your colleague is probably not your wife or your husband. But you are all involved in the same company, like in the same family, and that's the problem, because sometimes things can be broken, because somebody considers that he's not a part of the family.

**MARTIN LESSER:** In the future, for many companies that will no longer be a real problem, because biometric systems will replace password systems, so it's only a question of a few years, before we have fingerprint scanners.

**MICHEL YARHI:** We don't have very much time, and we have two more topics. 'Creating an operating environment that manages and mitigates risk'. Something easy, you all practice this kind of thing.


**JEAN-MICHEL PARIS:** Maybe as risk professionals, the idea should be to challenge a few key things. It goes back to your initial risk identification, your risk assessments, but then, if you find that there are things that you really need to get on top of, this is where you say 'I want to see this, because this is the right mitigating procedure'. So, for example, in the IT world you would probably say 'There is an environment in which you need to develop the new pieces of software that you will need', and then I want to see that clearly separated from the actual operating environment, so I want formal procedures for the go- lives. I want to have two different teams doing it, and we will not give the green light unless we have seen this, this, this and this, and it has been documented, and so on and so forth'. You can always find things to say as a risk professional, even if you don't fully understand the intricacies of the technical subject.

**MICHAEL ROSSI:** The thing that I've seen as best practice, as has already been mentioned, and it's interesting how many of my clients don't do it, is where the risk manager and IT are coming together and intertwining the two disciplines. So that jointly a group can decide 'Well where are we going to put money for loss control, risk control, and where are we going to insure it?', because trying to insure these risks is impossible for the risk manager to do without the help of IT, because you have to go through security audits, you have to fill out insurance applications. But there also has to be the decision, the joint decision, Where are we going to spend insurance premium, dollars on these risks? And it should turn out to be on the low frequency high severity ones. But without input from IT, the risk manager is just going to be swimming in a sea of not having enough knowledge. To me that is the best practice; that's the team approach; it sounds like you've been doing that. It is just interesting how many companies don't do it, and where their risk manager is all alone trying to figure out what to insure or not insure, without any help from IT department. It's getting better. Five years ago it used to be that IT departments in a lot of companies were 'Don't come and talk to

**I DON'T CARE HOW MUCH MONEY YOU PUT INTO RISK MANAGEMENT, THE LOSSES WILL STILL HAPPEN**
**MICHAEL ROSSI**

me, I'm an island unto myself, don't ask me any questions about our security, because why am I going to tell you? and why am I going to tell an underwriter where our weaknesses are, because then we can just be exploited by someone else?' That's getting better, and that's because I think more and more risk managers are making the entrée into the IT department, 'let me partner with you', it's all about how you communicate with the IT department 'I'm not here to look over your shoulder, I'm here to partner with you and, as a team, we're going to develop a strategy that benefits the company'. That to me is the best practice.

**MICHEL YARHI:** Okay, so we are into the last quarter of an hour, with just time for the last item. ' Protecting against external threats, such as viruses and against attacks and internal security threats'.

**IT'S YOUR INSTANT RESPONSE THAT ACTUALLY DECIDES WHETHER YOU SURVIVE OR WHETHER YOU DON'T SURVIVE: IT'S THE RESPONSE THAT IS GOING TO SAVE YOUR REPUTATION**
**ANDY BULGIN**

**PASCAL LOINTIER:** May I start?. First, you quoted viruses as being people's first nightmare. Our computer security association periodically does a security assessment at a national level. In the previous survey it looked at, viruses were the big nightmare for people, but they also understood that viruses were not very damaging to their system. So there is a bit of contradiction, because they were afraid of viruses, but they knew that they did not have the greatest impact for potential losses. Possibly it was due to the hype in an IT magazine regarding love letter viruses and so on. Now, even in your study, people are still afraid of viruses, but viruses do not behave as they did in the past. In the past they were just deleting data off documents. Now there is perhaps reduction or dysfunction of the network, or disabling laptops and desktops, but not destroying data, as they have done in the past, and as they could do in the future.

**MARTIN LESSER:** In the meantime, hacking has become commercial; there are many people world-wide who operate on so-called botnet, so there are thousands of computers which are under the control of a single person and which can be used to attack your company. If a botnet, for example, 20,000 or 30,000 computers, is attacking your net, then you will have trouble. At the moment, we are talking about two million computers online world-wide, which are controlled by third party hackers. That's the current number.

**MICHAEL ROSSI:** I think what Martin has said is something I agree with, and, again, I'm probably outside here, but I don't care how much risk management you put into protection of the data and protection of the integrity of the system, the risk is still there. Theft of the data; systems going down. And we continue to see losses, some of which aren't reported specifically, and we see cyber extortion, because people don't want to go out and report publicly that they're victims. But we've seen losses from cyber extortion in a 10 million $US range; we've seen losses from viruses in the 14 million $US range, and losses, because of employee malicious destruction of data, in the 50 million $US range. Now I don't care how much money you put into risk management, the losses will still happen. And to me the bigger question is, assuming that losses will happen, do you insure it or not? And some people have very very strong feelings about that. Some people say no, because if a loss is going to happen on the first party side, I'm only insuring catastrophic, 50, 100, 150 million. You can't buy that. On the liability side 'Well it's insured, either because I've got libel and slander coverage, or pure financial loss coverage'. And to me those are the really difficult issues, it's what's already insured, what's not, and how you separate them, and, as to what's not already insured, are the risks severe enough to go and insure it? The only thing you can assume is the risks are going to happen no matter how much you manage them.

**MICHEL YARHI:** If I can take a banking approach, I would say the insurance problem is not the real issue. If, for example, somebody set up a phishing activity; if somebody broke the access to the credit cards, it's not a problem of insurance; it's a problem of the confidence of the customer towards the bank. If the confidence of the customer fails, he can close the bank; it's not a problem of insurance. So for us, the most important thing is to avoid any kind of attack and, if there is an attack, to limit it.

**ANDY BULGIN:** Yes, I think your second point is the most valid, because if you look at almost every major issue that happens from a risk management perspective, it's your instant response that actually decides whether you survive or whether you don't survive: it's the response that is going to save your reputation. Now, maybe you take a financial hit and maybe you manage to recoup some of that back from insurance, but ultimately that's a sticky plaster that goes on one side. But what you actually do to maintain the reputation of your bank or what we do to maintain the reputation of our beverages business, is what's actually tantamount to your future survival in business. I think a second thing here is that we're talking about protection of data. I think a lot of people don't actually understand the implications of the sensitivity of data that they're actually holding, and, if you're looking from the point of view of personal information held on employees, for example, it's a huge issue in the States, the theft of personal information, identity theft and the like. That's the kind of thing that I think many professionals within our businesses are not necessarily aware of the implications, the cost to the organisation of the theft of that kind of data. And that's probably where we should be trying to focus, to make people aware of what's going to happen if that data goes, because it may be a lot more sensitive than pure corporate information.

PPA INTERNATIONAL BUSINESS AND PROFESSIONAL MAGAZINE OF THE YEAR

StrategicRISK

# EURO FORUM
# LES CYBER-RISQUES
# PARIS

EN PARTENARIAT AVEC

CERTAINS DISENT QU'UNE SEULE DÉFAILLANCE TECHNOLOGIQUE PEUT MENACER UNE ENTREPRISE. D'AUTRES QUE L'INCAPACITÉ À S'ADAPTER PEUT ENTRAÎNER SA FAILLITE. NOUS, NOUS VOUS DISONS : RESTEZ CONNECTÉS !

Nous ne reculons pas devant les risques, nous les maîtrisons. Nous assurons l'innovation et sécurisons les réseaux de votre entreprise contre les risques liés aux technologies de l'information. L'offre Dataguard™ vous propose des solutions complètes d'assurance du risque informatique pour protéger tous vos systèmes d'information numériques. Pour plus d'informations, veuillez contacter François Fournié au 01.55.91.45.07 ou visitez notre site Web à l'adresse suivante : www.acelimited.com pour en savoir plus sur nos assurances et réassurances internationales.

ace group

ASSURONS LE PROGRÈS℠

# Introduction

# Les Risques informatiques majeurs

L'importance du cyber-risque ne diminue pas avec le temps, elle continue au contraire à progresser dans l'ordre des priorités des risk managers, suivant en cela la dépendance des entreprises envers des systèmes potentiellement vulnérables et qui sont confrontés à des menaces liées aux nouvelles habitudes de travail. Au cours de notre première session Euro forum, les participants avaient débattu autour des résultats d'une étude, menée par StrategicRISK en association avec ACE, qui observait les cyber-risques majeurs rencontrés par les organisations européennes.

Sept sujets ressortant de cette étude avaient été sélectionnés par StrategicRISK dans la mesure où ceux-ci offraient de bonnes perspectives de discussion. Parmi ces sujets figuraient : l'amélioration des processus informatiques et la mise en conformité avec les normes réglementaires, le maintien du contrôle sur la sécurité de l'information et la protection contre les menaces externes et internes.

Parmi les points essentiels qui émergèrent du débat figuraient l'impérative nécessité d'une bonne communication entre les risk managers et les services informatiques, les difficultés de la sensibilisation à la sécurité au sein des organisations et le fait que la vulnérabilité par rapport au vol ou à la perte de données peut provoquer non seulement des pertes financières mais également des dommages potentiellement irréparables à la réputation d'une organisation.

**Andrew Leslie**
Deputy Editor
StrategicRISK

## Participants à la table ronde Euro Forum Paris

**Michel Yarhi**
**Directeur des assurances du groupe Société Générale et Président de l'AMRAE, présidait le débat.**

**Andy Bulgin**
**Directeur des Risques, Coca-Cola HBC sa**

**Gilbert Flepp**
**Directeur des lignes techniques pour l'Europe continentale chez ACE European Group Ltd**

**Daniël Jacobs**
**Souscripteur lignes techniques de la branche Dommages aux biens et aux personnes chez ACE European Group Ltd**

**Martin Lesser**
**Consultant en sécurité informatique, Bettercom**

**Pascal Lointier**
**Président, CLUSIF**

**Jean-Michel Paris**
**Corporate Risk Manager, Bureau Veritas**

**Patrick Pouillot**
**Directeur de la souscription risques informatiques pour l'Europe continentale, ACE European Group Ltd**

**Fabrizio Sechi**
**Business Security Planning Manager, Fastweb**

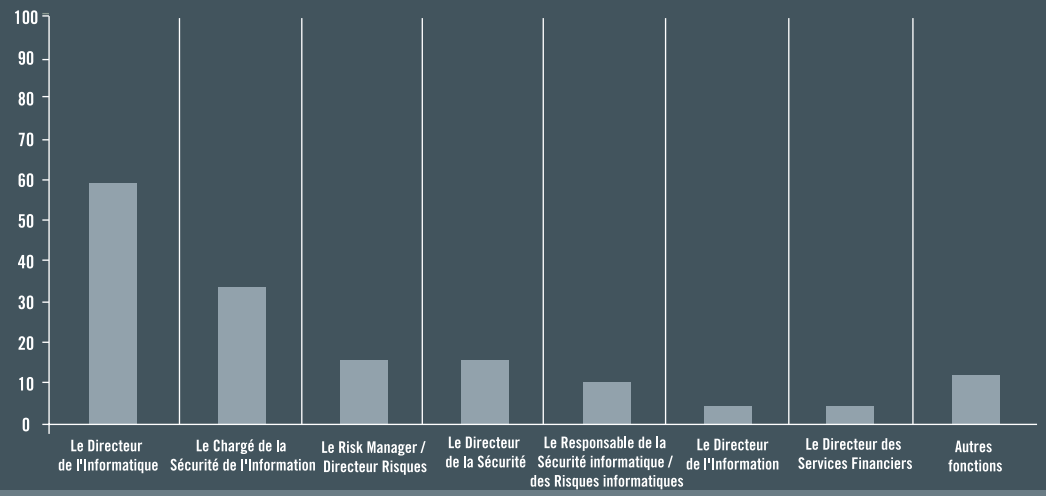
**Olivier Sorba**
**Directeur des risques, Groupe Lagardère**

**Patrick Smith**
**Directeur Europe, Gestion des sinistres et des risques, Hertz Europe Ltd**

**Michael Rossi**
**Président, Insurance Law Group**

# Rapport de synthèse

## La sécurité informatique est souvent sous la responsabilité du Directeur de l'Informatique ou du Responsable de la Sécurité




### Qui est responsable de la sécurité informatique ?

| | | | | | |
|---|---|---|---|---|---|
| Le Directeur de l'Informatique | 59% | Le Directeur de la Sécurité | 4% | Le Directeur des Services Financiers | 4% |
| Le Chargé de la Sécurité de l'Information | 33% | Le Responsable de la Sécurité informatique / des Le Directeur de l'Information | 16% | Autres fonctions | 2% |
| Le Risk Manager / Directeur Risques | 16% | Le Risk Manager / Directeur Risques | 10% | | |

À noter : le pourcentage total dépasse 100 %, les sondés pouvant choisir plusieurs réponses

Durant la fin juillet et le mois d'août 2006, l'équipe de recherche de Strategic RISK a conduit une cinquantaine d'interviews structurées auprès de personnes responsables de l'informatique ou du risk management dans 48 entreprises et organismes publics européens. Le but de cette étude était de cerner les approches de ces diverses organisations en ce qui concerne les risques liés à l'informatique – tant les risques internes qu'externes – et d'évaluer la fiabilité de leurs systèmes de défense.

Quels sont les enseignements de cette étude ? Que nombre d'entreprises, y compris parmi les plus grandes, ne disposent pas d'une bonne maîtrise de leur risque informatique. 16 % des personnes interrogées – y compris dans certaines multinationales – pensent en effet que leur société n'a que partiellement identifié les risques informatiques. Nous avons par ailleurs constaté que de gros efforts sont consentis dans ce domaine. Grâce à l'évolution rapide des technologies et, dans une certaine mesure, en raison des fusions et acquisitions, l'identification des risques est désormais perçue comme un processus permanent. Même si la détection des risques liés à l'informatique reste souvent l'apanage des responsables TIC et des risk managers, nombre d'autres services y contribuent désormais.

### Perception et réalité du risque

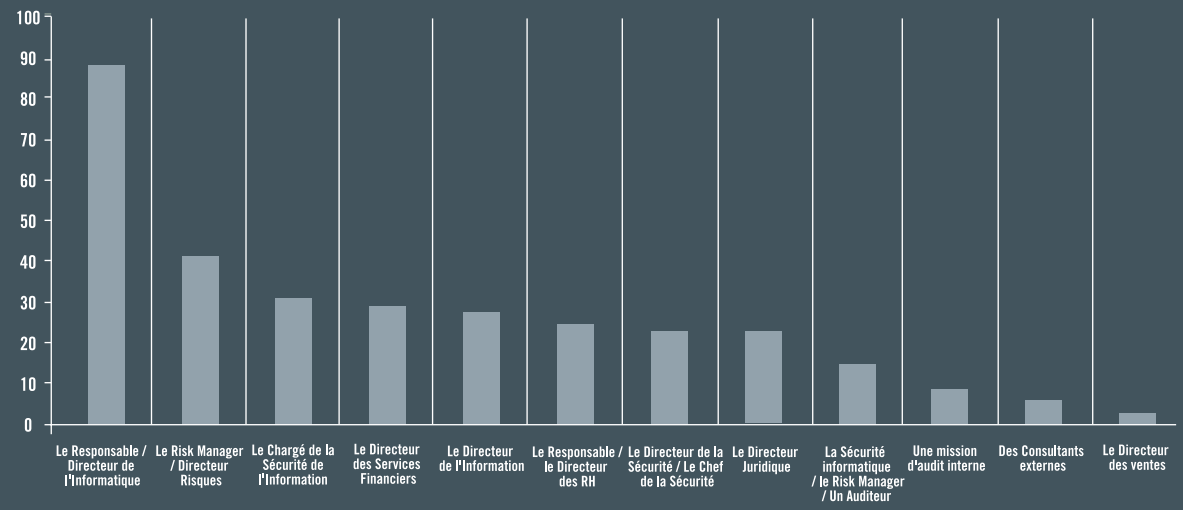
Où sont les vrais risques ? La plupart des sociétés considèrent que les virus représentent la principale source de risque externe, suivie immédiatement par le vol ou la divulgation de données confidentielles. Parmi les autres risques externes, on cite la dissémination d'informations confidentielles et le piratage. Les tentatives d'extorsion suite à un vol de matériel ou de données arrivent en bas de liste. Par contre, les risques liés à des catastrophes telles que les incendies, les inondations, les cambriolages, les pannes matérielles ou encore les pannes logicielles sont considérées comme de réels dangers.

En ce qui concerne les risques internes, les erreurs de manipulation arrivent en première place, suivies de près par le vol par un employé ou le détournement de données. La possibilité de voir un employé quitter la société en emportant des fichiers est une question qui préoccupe nombre de responsables.

Les entreprises semblent particulièrement vulnérables sous certains angles. La plupart de leurs plans de prévention ou de limitation des risques externes tournent autour des questions de virus, de piratage ou d'interruption de l'alimentation électrique. Les problèmes d'attaque par déni de service (DOS), la diffamation, l'atteinte au copyright ou encore la dissémination d'informations confidentielles sont moins bien couverts. Les défenses contre l'extorsion après un vol de données ou de matériel et les autres types d'attaque, de vol ou d'utilisation malveillante des données sont quant à eux les parents pauvres. Pourtant, le risque le plus réel encouru par la majorité des entreprises n'a rien de high tech : il s'agit tout simplement du vol de mots de passe, d'agissement illicites de société tierces et – pire encore – de l'absence de procédures de sécurité chez les partenaires et prestataires en informatique. Certains organismse ne disposent d'aucune protection dans ce domaine.

En ce qui concerne les risques internes, la plupart des entreprises tachent de

## Les informaticiens et les risk managers s'occupent le plus souvent d'identifier les risques informatiques




### Qui a travaillé à l'identification des risques informatiques ?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Le Responsable / Directeur de l'Informatique | 88% | Le Directeur des Services Financiers | 29% | Le Directeur de la Sécurité / Le Chef de la Sécurité | 22% | Une mission d'audit interne | 8% |
| Le Risk Manager / Directeur Risques | 41% | Le Directeur de l'Information | 27% | Le Directeur Juridique | 22% | Des Consultants externes | 6% |
| Le Chargé de la Sécurité de l'Information | 31% | Le Responsable / le Directeur des RH | 24% | La Sécurité informatique / le Risk Manager / Un Auditeur | 14% | Le Directeur des ventes | 2% |

À noter : le pourcentage total dépasse 100 %, les sondés pouvant choisir plusieurs réponses

minimiser les conséquences potentielles d'une panne de secteur ou d'une malveillance de la part d'un employé. Par contre, une majorité d'entre elles n'ont, de leur propre aveu, que peu de marge de manœuvre en ce qui concerne les erreurs de traitement, les malveillances internes, le vol ou le mauvais usage de données, la perte ou les dommages sur des d'équipements ou les erreurs humaines.

Les sociétés mettent en œuvre toute une palette de stratégies et de techniques pour minimiser les conséquences d'actions malhonnêtes ou négligentes ainsi que celles de l'incompétence ou de la malveillance. De plus, les entreprises pour lesquelles les questions de sécurité sont primordiales tendent à mettre des procédures de sélection du personnel plus rigoureuses (vérification des antécédents judiciaires) ainsi qu'une formation et un suivi plus pointu.

Dans la pratique, il ressort de l'étude que la principale cause de problème informatique sur les 12 derniers mois est l'erreur humaine. La cause suivante était l'interruption de l'alimentation électrique.

**Accès à distance, fraude et assurance**

La plupart des entreprises autorisent certains de leurs employés à accéder à leurs serveurs à distance. Dans les grandes sociétés, la sécurité de ces accès à distance est traitée avec le plus grand sérieux. Par contre, les entreprises plus petites ou plus anciennes paraissent particulièrement vulnérables. La plupart des organisations autorisent les accès à distance : outre l'encadrement supérieur, le personnel des services informatiques, les cadres moyens et certaines fonctions de terrain peuvent accéder aux serveurs.

Les cas de fraude informatique constituent un réel problème. Une personne interrogée sur sept a indiqué que son entreprise avait subi une fraude informatique durant les 12 mois écoulés. Dans trois de ces cas, le préjudice était inférieur à 500 000 euros, mais dans quatre autres cas, les pertes s'élevaient entre 1 et 5 millions d'euros.

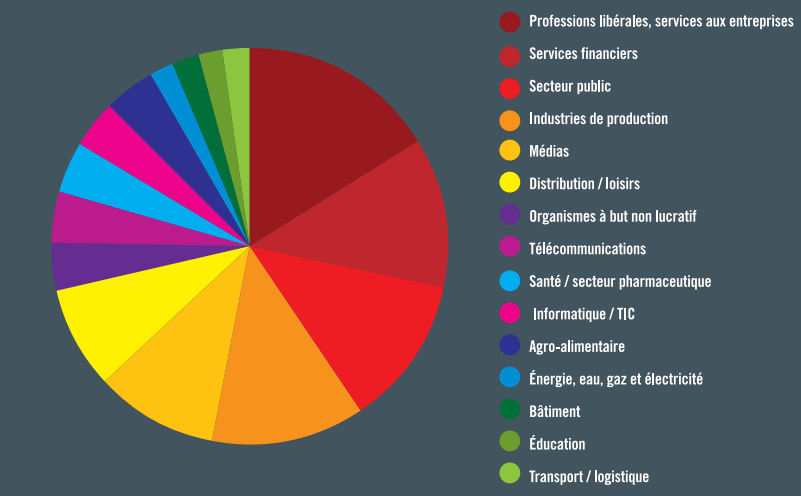
Il est relativement rare que les entreprises soient couvertes par des polices d'assurance couvrant spécifiquement les risques informatiques. Pour couvrir ce type de risques informatiques, les sociétés se contentent le plus souvent de la couverture offerte dans le cadre de leur police d'entreprise pour les dommages et la perte d'exploitation. Nombre de responsables souhaitent davantage de clarté, d'information et de conseil à ce sujet.

Dans l'ensemble, seul un quart des responsables interrogés jugent que leur entreprise dispose d'un système de risk management et d'un plan de continuité d'activité "tout à fait efficace". La plupart des sociétés jugent que les leurs sont "plutôt efficaces". Il reste cependant 6 % des entreprises qui considèrent que leur préparation est "plutôt inefficace" sur le plan informatique et 10 % qui jugent de la même manière leur plan de continuité.

Enfin, le risk management en informatique et les plans de continuité sont des sujets brûlants : nombre de personnes interrogées – dont une partie étaient des responsables risques récemment embauchés – sont conscientes de la masse de travail qui leur reste à effectuer au sein de leur entreprise pour mettre en place des systèmes de protection adéquats.

# Profil des personnes interrogées

## Les sondés proviennent d'une variété de secteurs

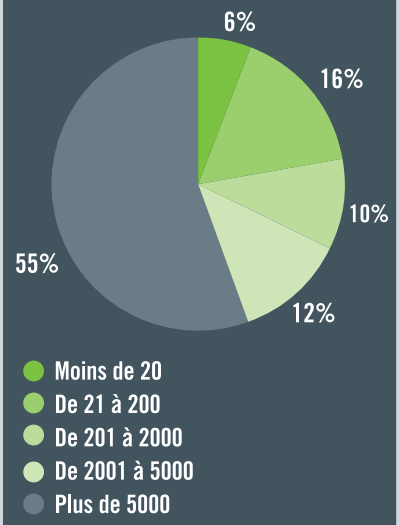



### Répartition des sondés par secteur d'activité

| | | | |
|---|---|---|---|
| Professions libérales, services aux entreprises | 16% | Santé / secteur pharmaceutique | 4% |
| Services financiers | 12% | Transport / logistique | 4% |
| Industries de production | 12% | Informatique / TIC | 4% |
| Médias | 12% | Agro-alimentaire | 2% |
| Secteur public | 10% | Énergie, eau, gaz et électricité | 2% |
| Distribution / loisirs | 8% | Bâtiment | 2% |
| Organismes à but non lucratif | 4% | Éducation | 2% |
| Télécommunications | 4% | Total | 98% |

À noter : en raison des arrondis, le total n'est pas égal à 100 %

## La plupart des sondés représentent des entreprises de plus de 5000 salariés




### Nombre d'employés dans l'entreprise du sondé

| | |
|---|---|
| Moins de 20 | 6% |
| De 21 à 200 | 10% |
| De 201 à 2000 | 55% |
| De 2001 à 5000 | 16% |
| Plus de 5000 | 12% |
| Total | 99% |

À noter : en raison des arrondis, le total n'est pas égal à 100 %

**Les secteurs d'activité**

Le groupe de personnes interrogées le plus représentatif est celui des "professions libérales / services aux entreprises" avec 16 % des réponses. Les services financiers, les industries de production et les médias représentent pour leur part 12 % des réponses, le secteur public 10 % et la distribution / loisirs 8 %. Le reste des interviewés se répartit entre divers secteurs : télécoms, transport, pharmaceutique, informatique, agro-alimentaire, énergie, bâtiment, éducation et organisations à but non lucratif.

**Répartition des organisations par taille et par C.A.**

Le nombre de salariés dans les entreprises interrogées s'étage d'une dizaine à plusieurs dizaines de milliers. La plupart emploient plus de 5000 personnes.

Le groupe le plus représenté parmi les interviewés est celui des entreprises dont le chiffre d'affaires est compris entre 50 millions et 1 milliard d'euros (33 % du total). 46 % des entreprises interrogées affichaient par ailleurs un C.A. supérieur à 1 milliard d'euros et 22 % parmi elles indiquaient plus de 5 milliards d'euros. Quelques-unes de ces entreprises opèrent dans des secteurs tels que la finance, le traitement des paiements, la sécurité, l'information sur la solvabilité ou les contenus numériques ; pour elles, la sécurité informatique est cruciale et elles emploient souvent des dizaines – voire des centaines – de salariés à la garantir. Les autres entreprises considèrent plutôt la sécurité informatique comme une question de routine.

**Vendez-vous des produits ou des services au travers d'un site Internet ?**

Nous avons demandé aux interviewés si leur entreprise vendait des produits ou des services par le biais d'une plate-forme en ligne. 51 % d'entre eux ont répondu positivement. Si l'on élimine les cinq services publics interrogés, le total ne s'élève alors guère qu'à 52 %, dans la mesure où 2 des 5 services publics vendent sur Internet.

**Vendez-vous des produits ou des services au travers d'un site Internet ?**

| | |
|---|---|
| Oui | 51 % |
| Non | 49 % |
| Total | 100 % |

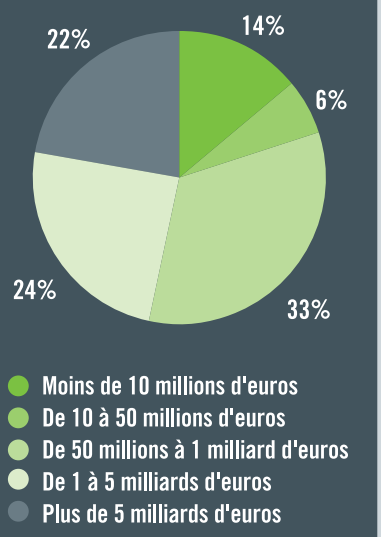
**Si la réponse est oui, s'agit-il de commerce entre entreprises (B to B) ou avec le consommateur final ?**

Sur les 25 structures interrogées vendant des produits ou des services par le biais d'un site marchand en ligne, 5 d'entre elles ne vendent qu'aux entreprises et 5 autres ne vendent qu'aux particuliers. Les 15 restantes (soit 60 %) vendent aux deux clientèles.

**La vente en ligne sur votre site vous conduit-elle à recueillir des informations personnelles telles que des numéros de carte bancaire ou des adresses ?**

Bien que seulement 51 % des entreprises interrogées vendent des produits ou des services en ligne, 59 % des interviewés ont indiqué qu'ils recueillaient des

**Le chiffre d'affaires de la plupart de ces entreprises dépasse le milliard d'euros**

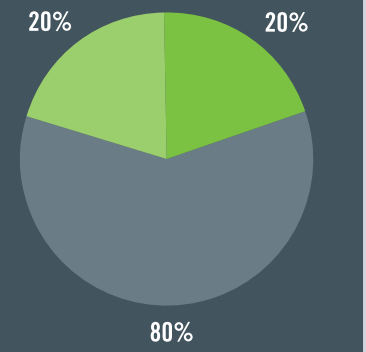



**Chiffre d'affaires de l'entreprise du sondé**

| | |
|---|---|
| Moins de 10 millions d'euros | 14% |
| De 10 à 50 millions d'euros | 6% |
| De 50 millions à 1 milliard d'euros | 33% |
| De 1 à 5 milliards d'euros | 24% |
| Plus de 5 milliards d'euros | 22% |
| Total | 99% |

À noter : en raison des arrondis, le total n'est pas égal à 100 %

**6 serveurs en ligne sur 10 gèrent des transactions B to B et avec le consommateur final**




**S'agit-il de commerce entre entreprises (B to B) ou avec le consommateur final ?**

| | |
|---|---|
| Business to Business (B to B) | 20% |
| Avec le consommateur final | 20% |
| Les deux | 60% |
| Total | 100% |

informations personnelles provenant des visiteurs de leur site. Dans certains cas, il ne s'agissait cependant que de données peu confidentielles, destinées à valider l'inscription à un bulletin d'information en ligne ou le téléchargement d'un CV.

**La vente en ligne sur votre site vous conduit-elle à recueillir des informations personnelles telles que des numéros de carte bancaire ou des adresses ?**

| | |
|---|---|
| Oui | 59 % |
| Non | 41 % |
| Total | 100 % |

**Votre entreprise dispose-t-elle d'un intranet et/ou d'un extranet et autorise-t-elle l'utilisation d'ordinateurs portables de l'entreprise pour le télétravail ?**

94 % des organisations interrogées disposent d'un intranet. Seules 6 %, soit trois entreprises, n'en disposent pas. Ces trois entreprises ont un effectif inférieur à 200, d'eux d'entre-elles ayant de moins de 20 employés.

En ce qui concerne l'extranet, deux tiers des organisations en sont équipées. Parmi celles qui n'en sont pas dotées, 80 % sont des entreprises publiques mais 13 % seulement sont des entreprises réalisant un C.A. supérieur à 1 milliard d'euros.

Les ordinateurs et autres équipements électroniques portables sont maintenant omniprésents, ce qui, on le verra, n'est pas sans créer quelques problèmes de sécurité spécifiques. Une des entreprises interrogées indique qu'un tiers de son effectif travaille la plupart du temps à distance, chez les clients : "Nous avons 60 succursales disséminées dans 23 pays. Nos employés peuvent se connecter dans n'importe laquelle." Seule une entreprise interrogée a indiqué que personne au sein de la structure n'utilisait d'ordinateur portable pour travailler hors des bureaux.

Si vous souhaitez recevoir l'intégralité du rapport de recherche portant sur les risques liés à l'informatique (sur fichier informatique), veuillez contacter Patrick Pouillot, le Directeur de la Souscription des risques informatiques pour l'Europe continentale à l'ACE European Group Ltd au numéro : + 33 01 55 91 45 45 ou bien par courriel à l'adresse : patrick.pouillot@ace-ina.com

# Table Ronde sur les Risques Informatiques

**MICHEL YARHI:** Je crains que nous ayons moins de deux heures pour traiter les sept sujets différents soumis par Strategic Risk. Ceci ne nous laisse que peu de temps, environ un quart d'heure pour chaque sujet. Si vous le souhaitez, nous pouvons les prendre un par un, essayer d'apporter quelques réponses d'après nos expériences sur le terrain et discuter de la manière de gérer les différentes formes de risques. Le premier sujet proposé concerne l'amélioration des processus informatiques et la mise en conformité avec les normes réglementaires. Qui peut nous faire part de son expérience sur le sujet pour lancer le débat ?

**PATRICK SMITH:** Puis-je vous parler de Hertz ? Je dois commencer par vous dire que je suis arrivé récemment chez Hertz et que c'est également ma première expérience dans une entreprise de taille mondiale. Ainsi, une partie de ma préparation pour cette table ronde a consisté à trouver qui était responsable de ce domaine, bien que cette responsabilité me revienne partiellement : j'ai finalement appris que c'était sans doute une personne travaillant à Oklahoma City, où ils passent le plus clair de leur temps à contrôler des données, mais que cette personne était en vacances en ce moment. Ma préparation a donc été difficile. En général, j'observe que nous avons des règles de sécurité informatiques strictes. Nous avons une protection par mot de passe qui fonctionne presque en temps réel : si vous quittez votre poste de travail, votre écran se verrouille et, si je travaille depuis mon domicile, j'ai une chance sur deux de me connecter, non parce que j'aurais commis une erreur de manipulation, mais parce qu'il existe une procédure intégrée qui a pour principe "ne leur facilitons pas les choses." Dans ce cas, un numéro d'assistance me met directement en

relation avec Oklahoma City, où mon accès est alors validé. C'est comme pour appeler ma banque : ils me demandent mon code postal, ma taille, ma date de naissance et ils me rendent mon mot de passe. Nous avons donc une approche très stricte de la sécurité informatique, servie par…

**MICHEL YARHI:** Excusez-moi de vous interrompre, ces règles sont-elles spécifiques à société, officialisées et applicables par tous les collaborateurs ?

**PATRICK SMITH:** Je reçois chaque jour, de la part de notre département des procédures, une moyenne de trois notifications, qui concernent parfois de nouvelles procédures et le plus souvent des modifications. Il est très difficile de distinguer les notifications pertinentes de celles qui ne le sont pas. Ce qui maintient la cohésion de l'ensemble, c'est la

## ÇA PEUT CONDUIRE À UNE PARALYSIE PROCÉDURIÈRE

**PATRICK SMITH**

conformité SOX (Sarbanes-Oxley). Cela conduit à un environnement dans lequel les gens passent systématiquement par des sas de vérification, alors que je viens de structures plus réduites où chacun navigue à l'estime. Ce mode de fonctionnement comporte des risques, mais il faut également faire attention avec les systèmes de vérification systématique, parce que personne ne parvient à mémoriser 3000 procédures en même temps. Mais c'est une façon de travailler. Le seul risque que je vois à cela est que la fiabilité de notre approche des risques externes ca peut conduire à une paralysie procédurière. On

## IL EXISTE UN DÉBAT DE FOND SUR LE TRAITEMENT DES DONNÉES PERSONNELLES

**OLIVIER SORBA**

se demande parfois à quelle heure de la journée on va bien pouvoir commencer à travailler.

**MICHEL YARHI:** Quelle est l'expérience des autres participants ? Je suppose que chaque entreprise dispose de règles internes de sécurité informatique, alors quel est le niveau de contrainte imposé par ces règles ? Sont-elles très contraignantes ? Comment les vivez-vous ?

**ANDY BULGIN:** Je pense que cela dépend énormément du type d'entreprise en termes de flexibilité et d'autonomie des unités d'exploitation. Si vous observez Coca Cola HBC, nous avons un schéma directeur central, mais un degré d'autonomie opérationnelle au niveau de chaque pays. La question, quand vous appliquez cela dans un contexte informatique, est la suivante : est-ce que vous fixez comme règle absolue que chacun doive faire certaines choses, acheter certains systèmes, travailler de certaines manières, même au détriment de la rentabilité globale ? Ou bien instaurez-vous un degré de flexibilité dans le mode opératoire préconisé, au risque d'augmenter, bien sûr, le risque de non-conformité ou de préjudice à l'organisation ? Je pense que l'équilibre est difficile à trouver et, si l'on devait passer une heure par jour, comme je viens de l'entendre, à s'informer et assimiler des procédures en cours avant de pouvoir gérer ses impératifs opérationnels, alors je considèrerais cela comme un obstacle majeur. Si nous considérons que l'informatique doit avoir pour raison d'être l'accroissement de la performance et la productivité de chacun, il y a alors un conflit entre ces deux concepts.

**JEAN-MICHEL PARIS:** En termes de processus informatiques purs, je vais vous faire part de mon expérience au sein du Bureau Veritas. Nous avons décidé de scinder le département informatique en deux équipes : systèmes et logiciels. Ainsi, nous avons d'un côté une équipe centralisée qui surveille uniquement les infrastructures et les opérations, c'est-à-dire le matériel purement informatique, les liaisons, les connexions, les hubs et les centres de services partagés. De l'autre côté, une deuxième équipe supervise les applications en elles-mêmes. Les lignes de reporting sont intéressantes ici, parce qu'elles convergent au final vers le même responsable au niveau de la direction, mais par des canaux différents. Un tel schéma permet d'équilibrer les aspects purement techniques et applicatifs. La politique générale que nous appliquons provient de la combinaison des apports de ces deux entités. En termes de processus informatiques, la surveillance réciproque entre les deux equipes nous permet d'avoir une certaine tranquillité d'esprit.

**OLIVIER SORBA:** La question implique également la mise en conformité avec les normes réglementaires en vigueur, parce qu'il existe un débat de fond sur le traitement des données personnelles. La première question est : "Savons-nous exactement ce que dit la loi, ce que nous pouvons et ne pouvons pas faire ?" Le problème pour un groupe de dimension mondiale est que l'on se trouve confronté, au final, à des réglementations différentes selon les pays et que la question devient alors : "Qui est chargé de vérifier ?" Est-ce ce que les gens savent même qu'il existe des lois à ce sujet ? Je ne parle pour l'instant que du risque juridique, qui constitue en lui-même un sujet ?

**PATRICK SMITH:** Notre approche chez Hertz a consisté à utiliser un processus très restrictif et à l'appliquer au niveau mondial quel que soit le pays.

**OLIVIER SORBA:** Parfois, on n'a même pas le droit de détenir certaines informations. Même si l'on fait les choses en toute conformité, sans aucun pépin dans le système, il arrive parfois que le simple fait de relier deux fichiers vous mette dans l'illégalité. La compréhension des lois qui régissent ces procédures est un défi en elle-même.

**MICHEL YARHI:** Et le défi est encore plus grand pour les groupes de dimension mondiale, qui doivent s'adapter aux systèmes juridiques de chaque pays. Ce n'est pas facile. Autre chose à propos de la mise en conformité avec les règlements ?

**MARTIN LESSER:** Je voudrais savoir si, par exemple, les budgets de sécurité informatique sont en hausse pour cette année ou l'année prochaine, ou bien si vous les maintenez au même niveau que l'année dernière ou celle d'avant ?

**PATRICK SMITH:** Bonne question. Je ne connais pas la réponse. Il y a de nombreux chantiers de développement informatique et j'aurais tendance à croire qu'avec la complexification des systèmes, les coûts sont probablement plus élevés qu'il y a 10 ans. Il y a 20 ans, je me rappelle que le cyber-risque n'existait pas vraiment en informatique. Nous mettons en place en ce moment un nouveau système de gestion des réclamations par Internet qui offre de nombreux avantages pour nos clients, mais qui comporte également des risques inhérents qu'il faut contrer avec des dispositifs de sécurité. Ces dispositifs doivent être compatibles non seulement avec les exigences internes chez Hertz, mais avec celles de ses clients externes, qui ont leurs propres contraintes.

**MARTIN LESSER:** Je posais cette question parce que nous avons, en Allemagne, un bureau fédéral de la sécurité informatique qui a mené plusieurs études l'année dernière auprès de nombreuses entreprises. L'un des résultats de l'étude était que toutes les entreprises voyaient une augmentation des risques informatiques, mais que seules 39 % d'entre elles avaient augmenté leurs budgets de sécurité informatique. 40 % le maintenaient au même niveau que l'année précédente et les autres avaient en fait réduit ces budgets. Personnellement, je vois un nombre croissant de risques, surtout lorsque l'on pense à l'Internet. Nous constatons un saut qualitatif totalement nouveau dans les attaques. Il y a quatre ou cinq ans, les tentatives de piratage provenaient souvent d'adolescents boutonneux et c'était plutôt amusant, mais maintenant, ce sont de véritables organisations criminelles de Roumanie, du Brésil, de Chine et surtout de Corée, qui tentent de s'attaquer aux systèmes ; je vois personnellement les risques s'étendre pour toucher aussi les PME et non plus seulement les grands groupes.

**MICHEL YARHI:** Cela dépend aussi bien sûr de l'activité de chaque entreprise. Vous imaginez à quel point dans la banque, mon secteur d'activité, nous sommes concernés par la sécurité informatique en général, celle des logiciels et d'Internet en particulier. En effet, la plupart de nos clients ne se rendent plus dans les agences : ils font tout en ligne. Et si ce n'est pas sécurisé, nous sommes morts. Alors aujourd'hui la question la plus importante est : "Quel est le niveau de sensibilité au risque de votre entreprise ? Comment le gérer et comment le limiter ? Est-ce la première préoccupation de votre président ? Ou est-ce moins important ?" Je peux vous dire que pour nous, dans la banque, elle se situe en tête de liste de nos priorités, juste après les risques financiers, mais je suppose que c'est un sujet important pour chacun d'entre vous, n'est-ce pas ? Vous vous sentez contraints répondre par l'affirmative, parce qu'il y a des assureurs autour de la table. Bon, donc le premier problème se situe là…

**GILBERT FLEPP:** En ce qui concerne la mise en conformité avec les normes réglementaires en vigueur, est-ce que le

## LES ENJEUX SONT DE PLUS EN PLUS IMPORTANTS

**JEAN-MICHEL PARIS**

processus de mise en conformité a changé la perception du risque ou permis à votre organisation de mieux identifier des comportements frauduleux ou des domaines d'exposition au risque qui n'avaient pas été correctement évalués auparavant ?

**MICHEL YARHI:** Quelqu'un peut proposer une réponse ?

**OLIVIER SORBA:** Nous ne sommes pas certifiés SOX, c'est pourquoi je réponds. Il est vrai qu'il existe des réglementations moins contraignantes, mais ce genre de risques est apparu bien avant l'apparition des réglementations, comme sont apparus les efforts pour combattre ces risques. Nous sommes maintenant obligés de les combattre d'une manière très organisée et structurée.

**MICHEL YARHI:** De fait, nous n'avons pas besoin de SOX pour agir dans cette direction. Juste avant de venir ici, je préparais une autre conférence sur le contrôle interne. C'est là que réside le problème au quotidien : les contrôles internes doivent être mis en place dans

## ON N'AURA JAMAIS UN CONTRÔLE ABSOLU SUR LA SÉCURITÉ INFORMATIQUE

**MARTIN LESSER**

toutes les entreprises, non pas à cause de la SOX ou de toute autre contrainte, mais parce qu'il s'agit d'une question de vie ou de mort. Si vous ne maîtrisez pas votre risque, vous n'êtes pas viable : un simple virus peut vous mettre à genoux.

**JEAN-MICHEL PARIS:** Je pense que c'est de plus en plus vrai maintenant avec le nombre croissant de nos activités qui dépendent d'applications spécifiques. Ce n'était pas le cas auparavant. Avant, nous n'utilisions que des applications grand public comme Word, Excel ou autres, qui ne nécessitaient pas véritablement de développements particuliers pour des processus ou des prestations de services spécifiques. Maintenant, les applications de type ERP sont partout et on dépend d'elles pour les fonctions internes, tout comme d'autres applications, telles que PeopleSoft pour la fonction RH. Les principales fonctions internes de l'entreprise en dépendent donc et la marche de l'entreprise, quel que soit son domaine d'activité, dépend alors également d'applications spécifiques. Les enjeux sont de plus en plus importants. Quand vous demandez le degré de priorité de cet enjeu pour votre organisation, la réponse est sans doute très élevé et de plus en plus crucial.

**MICHEL YARHI:** Bien, la deuxième question concerne le maintien du contrôle sur la sécurité de l'information. C'est une question assez centrale. Qui conserve le contrôle ? Pascal, nous n'avons pas encore entendu l'avis de votre association. Avez-vous des informations sur vos membres ?

**PASCAL LOINTIER:** Pas encore, c'est vraiment une question de fonctionnement interne, je pense donc qu'il vaut mieux que les intervenants de chaque entreprise expliquent ce qu'ils font. J'ai recueilli quelques commentaires sur d'autres sujets mais pas sur celui-là.

**MICHEL YARHI:** Ok, donc pas de réaction sur ce sujet ?

**MARTIN LESSER:** Il y a un point particulièrement intéressant dans l'étude (de Strategic Risk) que j'ai lue hier. Toute personne qui a répondu aux questions sur les contrôles en affirmant avoir une confiance totale dans ces contrôles se berce d'illusions. Je pense que c'est très vrai. On n'aura jamais un contrôle absolu sur la sécurité informatique. À mon avis, les systèmes sont trop complexes. Il est impossible de tout contrôler.

**MICHEL YARHI:** Et parfois, le logiciel est si complexe que l'on utilise pas 100 % de ses capacités. On en utilise 50 %, 75 %, mais jamais 100 %. Quels sont les risques potentiels liés aux capacités inconnues et inutilisées des logiciels ? Ceci constitue vraiment un problème.

**MARTIN LESSER:** En matière de développement informatique, il y a une vieille philosophie appelée KISS – keep it small and simple (faites petit et simple). Mais aucun développeur de logiciel actuel ne s'en inspire. Ils essaient d'intégrer de plus en plus de fonctionnalités et chaque nouvelle fonctionnalité peut comporter de nouveaux risques.

**MICHEL YARHI:** Et comment sont les contrôles prévus pour limiter ce genre de risques ?

**ANDY BULGIN:** Je pense que tout le problème de la sécurité informatique réside dans le fait que la majorité d'entre nous ne comprend pas particulièrement bien l'informatique, parce que les professionnels de l'informatique parlent un langage different du nôtre. Donc, quand vous en parlez lors d'une procédure de contrôle, ou même dans un contexte SOX, lorsque l'équipe informatique vous dit qu'elle a mis en place certains contrôles, est-ce que les personnes qui en sont effectivement les garants sont qualifiés pour juger de la pertinence de ces contrôles ? Si nous ne comprenons pas comment fonctionnent tous ces systèmes, comment pouvons-nous être sûrs que nous exerçons les contrôles adaptés ? Et je pense que le contrôle, dans ces divers contextes, ramène toujours au comportement des individus au sein de l'entreprise. Vous ne pouvez contrôler ce que vous ne comprenez pas.

**MICHEL YARHI:** Avez-vous des personnes spécialisées dans les activités informatiques au sein des différents départements d'audit ? Parce que c'est un point crucial. Le département d'audit est-il capable de comprendre ce que nous faisons et comment nous le faisons ?

**JEAN-MICHEL PARIS:** Je pense que c'est un vrai défi pour les personnes chargées du risk management et de l'audit d'aller vers les spécialistes de l'informatique et de leur dire "Pouvez-vous prouver que ce que vous dites est vrai ?", et en faisant cela de manière à démystifier tout ce jargon informatique. Vous pouvez faire cela en interne ou missionner des personnes extérieures qui ont les compétences pour le faire, peu importe, mais je pense que le point essentiel réside dans votre capacité à remettre ou non en question les responsables informatiques. J'ajouterai que cette remise en question doit être perpétuelle, sinon cela devient un jeu de gendarmes et de voleurs… et on sait bien qui court le plus vite.

**PATRICK SMITH:** L'interface entre l'informatique et l'opérationnel est un défi crucial, ainsi que la question de la désignation des responsables. Il y a un risque à déléguer entièrement la fonction d'audit à des spécialistes car ils ne sont pas forcément des spécialistes du métier et que

l'un des principaux cyber-risques est lié aux erreurs de manipulation en interne par des non informaticiens. Si on laisse faire les spécialistes, on risque d'aboutir à une situation interdisant la moindre opération. Évidemment, la sécurité serait alors absolue ! Malheureusement, l'entreprise serait vite en cessation de paiement !. Je pense donc que le point de départ consiste à se demander ce que vous souhaitez que les opérationnels puissent faire avec le système informatique. Commencez par cela, plutôt que par l'aspect "que pourrions-nous faire avec notre système informatique". Il est cependant raisonnable, dans un environnement adéquat, d'avoir un spécialiste à la table. Je pense donc que la question est de réunir les personnes adéquates autour du projet. Si vous décidez que votre gendarme est l'audit interne, alors il doit comprendre quelles sont les réalités commerciales et en quoi consiste l'activité de l'entreprise.

**MICHEL YARHI:** D'autres commentaires sur la question ?

**OLIVIER SORBA:** Bien sûr, l'audit est important, mais je sens qu'il faut plus que cela. On peut demander aux informaticiens leur aide pour structurer notre regard sur les autres. Il faut se structurer, parce que le pilotage de grandes organisations transnationales se fait en mettant plus ou moins de pression sur le système. Les choses sont compliquées et on ne peut pas passer chaque détail au crible, mais on veut que des personnes compétentes le fassent et que la stratégie d'ensemble soit appliquée. Peut-on atteindre cet objectif par l'audit ? Mon sentiment est qu'il faut structurer les choses dans l'ensemble de l'organisation. L'audit y joue un rôle mais il n'y a pas que cela. Par exemple, une part importante du contrôle du risque réside dans la cohérence des choix de sécurisation au sein de l'organisation, on a donc besoin d'une stratégie et de communiquer sur ce thème. Il est évident que dans une banque cela doit être très strict, mais je pense que l'on peut décider en haut lieu que tous les clients autour du monde devront communiquer au travers d'une page Internet commune. Parfois c'est différent ; les gens font des métiers différents et ont des traditions diverses à travers le monde, il faut s'adapter.

**MICHEL YARHI:** Passons à la question suivante : comprendre les risques potentiels et communiquer sur ces risques auprès de la direction et des salariés.

**PASCAL LOINTIER:** J'imagine que chacun s'accordera avec l'idée que l'organisation et la gestion des hommes constituent des facteurs clés de succès en matière de sécurité informatique. Mais il faut avoir un certain sens de la psychologie. Si vous voulez convaincre une personne ou un groupe de personnes de faire quelque chose, il faut avoir quelques connaissances en matière de communication, de motivation et de comportement. Il faut savoir proposer à quelqu'un de faire quelque chose et trouver comment le convaincre de le faire. Ce n'est ni nouveau, ni magique, il s'agit seulement de communication. Si vous voulez communiquer avec vos collaborateurs, il faut maîtriser ces techniques, mais la plupart des responsables de la sécurité informatique et des administrateurs réseaux ne les connaissent pas ou ne pensent pas à les utiliser. Le résultat, c'est qu'ils établissent des règles, mais sans comprendre les motivations des personnes ni mesurer leur propension à accepter ces procédures. Je pense que c'est très important. Nous parlons tous du facteur humain, mais je n'ai jamais vu de responsables de la sécurité informatique ni d'administrateurs réseaux bénéficier de formation à la communication.

**MICHEL YARHI:** Et avoir une approche psychologique ?

**PASCAL LOINTIER:** Absolument ; les bons mots au bon moment et ainsi de suite. C'est de la manipulation, mais c'est de la bonne manipulation.

**DANIEL JACOBS:** C'est aussi une tâche très difficile. Si vous prenez par exemple le cas des clés USB : mes clients m'en envoient en gros une tous les quinze jours. Nous adorons ça ; on peut faire tenir toute sa base client sur une grosse clé USB et il n'y a plus qu'à la brancher. Jusqu'à présent, il n'existe pas de règlement nous interdisant leur usage, mais cela représente un risque potentiel : c'est très difficile à expliquer à tout le monde.

**PASCAL LOINTIER:** Si on prend les

**CELA REPRÉSENTE UN RISQUE POTENTIEL : C'EST TRÈS DIFFICILE À EXPLIQUER À TOUT LE MONDE**
**DANIEL JACOBS**

budgets, il y a des astuces possibles. Admettons que vous voulez quelque chose qui coûte 100 euros, vous dites "Ça coûte 150 euros" et quand on vous fait une objection, alors vous répondez "J'ai réussi à négocier et nous pouvons l'avoir pour 100 euros seulement" et les gens sont contents parce que vous avez fait baisser le prix. Je ne dis pas que ça marche à tous les coups, mais c'est un bon stratagème. C'est pareil quand vous essayez de convaincre les gens de faire quelque chose : il est préférable de les amener à y réfléchir plutôt que de les forcer à respecter des règles. Mais les informaticiens ne pensent pas à utiliser les artifices de communication pour faire passer ces connaissances et faire appliquer les stratégies.

**ANDY BULGIN:** On peut objecter à cela que les informaticiens ne devraient pas être responsables de la communication dans l'entreprise.

**PASCAL LOINTIER:** Pas de la communication en général, mais

**LES SALARIÉS SAVENT QUE LE TÉLÉCHARGEMENT PEUT CONSTITUER UN ÉNORME RISQUE POUR L'ENTREPRISE. MAIS ILS CONTINUENT À TÉLÉCHARGER**

**PATRICK POUILLOT**

communiquer sur des questions dans leur domaine, oui. En France, nous avons une charte des utilisateurs : les salariés doivent signer un document stipulant qu'ils ne serviront de l'Internet que dans le cadre professionnel. Au lieu de faire signer ce document aux salariés sans leur donner d'explication, il serait plus judicieux de leur expliquer pourquoi. Il n'est pas question de se transformer en gourou de la communication, mais seulement d'agir comme dans la vie privée.

**ANDY BULGIN:** Bien sûr, je comprends cela et je ne conteste pas le recours à la psychologie car il est plus raisonnable d'expliquer les choses et de convaincre les gens plutôt que décréter et d'imposer des règles. Mais la question réside plus pour moi dans l'intégration de l'informatique au sein d'un code global de conduite des affaires. Le lien n'est pas facile à opérer du fait de la mystification autour de la technologie, que les gens ne comprennent pas, mais si vous observez la gestion des risques en général, vous imposez à chaque salarié de l'entreprise un certain niveau de responsabilité personnelle et il devrait en être de même pour l'informatique. Revenons sur l'exemple des clés USB et poussons-le à l'extrême : si l'on considère que cet instrument représente un danger majeur pour l'entreprise, toute personne vue en train d'utiliser une clé USB devrait être sanctionnée, voire même licenciée. C'est très difficile à contrôler, mais s'il n'y a pas de sanctions, personne ne prendra le risque au sérieux.

**PATRICK SMITH:** Je suppose qu'il faudrait également une raison très valable pour interdire l'utilisation des clés USB au sein de l'entreprise. Si l'on parvient à démontrer où est le danger, le département informatique, comme tous les autres, comprendrait qu'il s'agit de supprimer un risque pour l'entreprise. Dans mes postes précédents, j'ai lutté pour faire en sorte que le département informatique comprenne la vocation de l'entreprise. Si on sent qu'ils ne sont pas de grands communicateurs, devons-nous pour autant arrêter de communiquer avec eux et les isoler ainsi encore plus du métier de l'entreprise ? Il y a augmentation du risque global lorsque nous nous reposons totalement sur les systèmes informatiques. Et le défi de l'entreprise est de s'assurer qu'aucun service ne soit isolé.

**JEAN-MICHEL PARIS:** Au sujet de la communication et des informaticiens, je voudrais les défendre un peu. Dans mon entreprise, il y a de fait un assez bon niveau de communication. Nous disposons d'indicateurs et de ratios de performances sur les durées de fonctionnement et d'arrêt technique, application par application, ainsi que nombre d'autres indicateurs chiffrés. Ils sont consultables par tous sur l'intranet, il vous suffit de cliquer dessus et vous pouvez les voir à tout moment de la journée. Je pense que le problème est le même pour toutes les fonctions de support : "Quel est votre degré d'implication dans votre métier ?"

**MICHEL YARHI:** Une réaction à ce propos ?

**PATRICK POUILLOT:** Juste un mot concernant la compréhension des risques potentiels. En tant qu'assureur, je pense que nous avons maintenant des couvertures standard pour les virus. Je pense que chacun comprend quels sont les risques posés par les virus et que les salariés savent que le téléchargement peut constituer un énorme risque pour l'entreprise.

Mais ils continuent à télécharger. Comprendre le risque potentiel n'est pas suffisant. Même lorsqu'on comprend le risque, on peut avoir un comportement qui devrait être interdit par l'entreprise. C'est comme cela que ça marche et c'est pour cela qu'il existe des compagnies d'assurance qui vendent des assurances informatiques. La compréhension n'est peut-être pas le mot clé. La façon dont nous réagissons en tant qu'entreprise à l'encontre des personnes qui téléchargent des fichiers de façon illicite est importante.

**MICHEL YARHI:** Si vous parlez d'assurance, puis-je vous rappeler que les assureurs ont fixé des franchises ? Il est

**NOTRE TRAVAIL CONSISTE À AMÉLIORER LA CULTURE D'ENTREPRISE EN TERMES DE SÉCURITÉ EN EXPLIQUANT QUE DES DÉFAILLANCES DANS LA SÉCURITÉ PEUVENT CAUSER DES PERTES**

**FABRIZIO SECHI**

dans l'intérêt des entreprises de ne pas avoir de problèmes et ainsi notre implication dans la sécurité contribue à la satisfaction de tous car nous diminuons le risque. Quand on est une grande entreprise et que la franchise est élevée, l'intérêt premier est de ne subir aucun sinistre. C'est la raison pour laquelle nous devons communiquer et, même si nous ne donnons pas tous les détails, chaque acteur doit jouer son rôle pour s'assurer que l'entreprise ne subisse aucun préjudice.

**FABRIZIO SECHI:** Chez nous, le problème central est un problème de culture d'entreprise. Comme nous sommes une société de téléphonie, nous avons de nombreux salariés qui travaillent dans les services informatiques et réseaux : ces gens-là accordent beaucoup d'importance aux sujets qui touchent la sécurité, la surveillance, la sécurisation technique. Notre principal problème se situe plutôt au niveau du département marketing et du service de la relation client, parce que la préoccupation de ces services n'est pas la sécurité. Leur préoccupation est de vendre ou de fournir la meilleure qualité de service à nos clients, le problème de la sécurité n'est donc pas un sujet important à leurs yeux. Notre travail consiste à améliorer la culture d'entreprise en termes de sécurité en expliquant que des défaillances dans la sécurité peuvent causer des pertes. C'est plus important à nos yeux que le meilleur des anti-virus ou le plus efficace des pare-feu. C'est un problème culturel, un problème fondamentalement culturel.

**ANDY BULGIN:** Je crois que ce dernier point est très intéressant car la cause de la majorité des problèmes, en termes de gestion des risques, est relativement facile à identifier : leur nombre est limité. En ce qui concerne l'informatique, il peut s'agir des actions de l'un de nos employés, 40 000 dans notre cas, ayant accès aux équipements. Si vous pensez, par exemple, que la panne de l'un de nos serveurs est l'un des plus gros problèmes qui peut survenir, je vous répondrais par la négative. Une telle panne ne serait probablement pas perçue comme un problème insurmontable… Par contre, je citerais la perte, dans un aéroport, d'informations confidentielles sur un ordinateur portable ou sur une clé USB. Sensibiliser 40 000 personnes aux conséquences de leurs actions et de ce qu'elles doivent ou ne doivent pas faire, est un énorme projet qui va vous coûter des millions en budget de formation. Beaucoup de gens vont rechigner à se former en minimisant le risque. Mais les conséquences sont potentiellement catastrophiques. Même si nous ne parlons pas ici d'informations hautement confidentielles sur nos clients. Nous détenons bien sûr quelques informations de cette nature, mais nous avons surtout les données personnelles de tous nos clients qui sont accessibles à l'ensemble de nos collaborateurs et il est pratiquement impossible, à mon avis, de superviser tout cela.

**LE NIVEAU D'ASSURANCE DE CE DERNIER EST MOINS ÉLEVÉ QUE LE RISQUE QUE NOUS PRENONS**
**MICHEL YARHI**

**MICHAEL ROSSI:** En tant qu'observateur et, je crois, étant le seul avocat à conseiller ici les compagnies sous l'angle de l'assurance, je voudrais ajouter que l'on pas encore évoqué le problème du vol de données. Ceci est arrivé à une société d'assurance bien connue aux États-Unis. Son serveur se trouvait dans une pièce où quelqu'un s'est introduit par le plafond, comme dans Mission impossible - ce n'est pas une blague ! Le serveur a été dévissé du sol, soulevé puis emmené. Mais c'est juste un exemple de ce qui n'a pas été discuté : le risque que représentent les locaux ainsi que leur sécurité. Les informaticiens ont tendance à penser tout de suite au piratage et aux choses de ce genre, mais tout le monde oublie la simple protection des locaux. Quid du vol des PC et de l'équipement en général ? Il me semble que quelqu'un doit en prendre la responsabilité et il faut que ce soit une personne du département Gestion des risques, son responsable, par exemple. Nous avons mentionné les droits de la personne et le risque de responsabilité légale qui l'accompagne. Mais ce n'est pas à cela que pensent les informaticiens, ils pensent au risque de perte que représente une panne du système, ou encore au vol de données qu'il faut ensuite reconstituer. Il faut pourtant que la protection de ces informations contre tous ces risques soit placée sous la responsabilité de quelqu'un qui pourra ensuite déléguer ou présenter un bilan de son action. En tant que juriste d'entreprises, je dirais qu'il faut parfois tâtonner un peu : il n'existe pas de solution globale à tous ces risques. C'est, selon moi, parce que le problème est encore récent.

**OLIVIER SORBA:** Cela nous renvoie à l'approche globale : la nécessité de réunir les responsables de la gestion des risques, où qu'ils se trouvent, et les informaticiens, pour étudier le risque que représentent les réseaux et leurs communications. C'est pour cela que les spécialistes risques et les spécialistes d'informatique doivent travailler ensemble. Vous êtes voué à l'échec si vous ne les réunissez pas. Encore une chose au sujet de la prise en main du projet. On finit toujours par demander aux gens de modifier leur comportement ou de dépenser de l'argent ; si l'équipe de direction ne s'engage pas dans cet effort, ce n'est même pas la peine de commencer. À la base, les informaticiens et les gestionnaires des risques, seuls, n'ont pas les moyens de demander aux gens de modifier leur comportement, leur façon de penser et autres. C'est pourquoi il est très important que la direction s'engage elle aussi pour assurer la réussite de l'opération.

**MICHEL YARHI:** Souhaitez-vous ajouter quelque chose ? Très bien, alors passons au sujet suivant : l'évaluation des fournisseurs de services informatiques en vue d'assurer leur conformité avec la politique de sécurité des systèmes.

**PASCAL LOINTIER:** Je ne fais pas appel à eux, personnellement, mais puis-je dire un mot ? Je crois qu'on fait trop confiance au nom et à la marque de son fournisseur sans évaluer, dans les faits, le contenu des accords ou la manière dont ceux-ci sont appliqués. J'ai entendu dire que certains fournisseurs ou centres de stockage des données n'appliquent pas les règles de sécurité prévues au contrat, en raison du coût que cela représente. C'est un peu comme si vous passez commande d'un extincteur, par exemple, et que l'on vous réponde: "Oui, on en a un", sauf que le jour où un incendie se déclare, il ne fonctionne pas et ils vous répondent : "D'accord, vous pouvez toujours nous faire un procès, mais vous savez qu'un procès en responsabilité ne vous rapportera pas grand chose comparé à son impact sur vos affaires" et c'est… Je ne dis pas que c'est le cas de tous les FAI et autres centres de données, mais ça arrive.

**MARTIN LESSER:** De plus, comment pouvez-vous être sûr que vos fournisseurs respectent votre politique de sécurité?

**PASCAL LOINTIER:** Il faut vérifier, prendre la décision d'envoyer quelqu'un pour faire un audit de leur système où le faire vous-même si vous en avez les compétences. Mais il faut que ce soit fait, vous ne pouvez pas vous contenter de ce que dit le contrat.

**MARTIN LESSER:** Il y a six mois, en Allemagne, nous avons eu un gros problème avec un prestataire qui travaille pour les sociétés vendant sur eBay. Il a été viré mais les données de grosses entreprises ont été volées, des mots de passe ont été changés, etc… Je ne pense pas que les sociétés clientes aient vérifié l'infrastructure ni surtout les logiciels, qui se sont avérés être non protégés. Mais je crois qu'il est particulièrement difficile de contrôler tous vos fournisseurs ainsi que leurs logiciels. C'est impossible. On peut faire quelques vérifications, quelques audits, on peut poser des questions, mais il est absolument impossible de tout vérifier en détail. Le risque subsiste toujours.

**ANDY BULGIN:** Je crois que le problème est double. D'une part se pose la question de la fiabilité technique de la personne à qui vous confiez vos données : son système va-t-il tenir ? Si ce n'est pas le cas, allez-vous récupérer vos données rapidement ? D'autre part, pouvez-vous avoir confiance dans la manière dont votre fournisseur gère des informations confidentielles pour votre compte ? Ce qui nous ramène à l'approche légale que vous avez mentionnée. J'ignore combien d'entreprises conduisent réellement des audits sécurité sur les tiers qu'elles

emploient. Si l'on effectue pas ces contrôles lorsqu'il s'agit de la production, on devrait probablement le faire lorsqu'il s'agit de la sécurité informatique d'informations confidentielles.

**PATRICK SMITH:** Pour moi, il s'agit d'un problème d'analyse coût/bénéfice. Il y a un logiciel qui va couvrir 80 % de mes besoins et j'ai donc besoin de couvrir les 20 % restant. Comment faire ? Mon approche, qui est celle adoptée chez Hertz, consiste à ne pas externaliser l'informatique. Nous nous procurons un logiciel extérieur, mais il est notre propriété, nous assumons les risques mais nous en tirons aussi les bénéfices. Il nous appartient, il est protégé par un contrat, par une licence d'utilisateur et tout ce qui s'en suit. Et toute la procédure d'acquisition et d'implémentation a fait appel aux compétences de l'équipe informatique pour s'assurer de sa sécurité… Je crois que l'idée est de ne pas s'en tenir à ce que nous dit le fournisseur : "Le système est-il sûr ? Oui, hyper-sécurisé. Ah, c'est super, merci." Je pense que nous devons être conscients de nos propres limites, nous devons essayer de trouver les solutions nous-mêmes et inviter nos amis informaticiens à nous aider. Et si nous parlons de culture, le fait, par exemple, de passer de produits faits maison à des produits pré-configurés, cela a été rendu possible par l'utilisation d'experts en informatique et de leurs compétences. Ils comprennent les paramètres et les risques liés aux questions de sécurité.

Je voulais aussi ajouter qu'une des raisons nous poussant à modifier le logiciel, un des avantages que nous en retirons, c'est la possibilité pour mon personnel de travailler différemment : c'est là, je crois, que réside l'un des risques nouveaux. Quand j'ai commencé à travailler, il était rare d'emporter du travail chez soi en fin de sa journée. Aujourd'hui, nous encourageons les gens à travailler chez eux, et c'est une très bonne chose. Nous encourageons nos clients à venir contrôler leurs informations, à effectuer leurs opérations en ligne. Nous pratiquons beaucoup cela dans mon entreprise, c'est logique sur le plan commercial. Toutefois, en tant qu'entreprise, nous devons garder à l'esprit les risques que nous créons nous-même. Je pense que l'un des avantages à monter une équipe de protection de l'entreprise, c'est que mes amis du service informatique ne sont pas abonnés à Strategic Risk : ils reçoivent par contre La Gazette des TIC où ils peuvent lire toutes sortes d'anecdotes sur des problèmes de nature informatique. Je n'y comprendrais rien, j'ai ma spécialité, ils ont la leur. Pourtant, si nous agissons ensemble, nous prendrons des décisions plus astucieuses.

**MARTIN LESSER:** Cependant, l'une des difficultés pour les responsables informatiques de grandes entreprises surgit lorsque le responsable de la gestion des risques leur demande s'il existe encore des problèmes. S'ils répondent qu'il en reste, leur crédibilité en souffre. Le danger est donc qu'ils répondent qu'il n'existe plus de difficulté pour ne pas perdre en crédibilité.

**PATRICK SMITH:** Souvent, cela dépend de la manière dont vous posez la question. En tant que responsable de la gestion des risques, je ne pense pas qu'il existe une réponse exacte. Soit le risque existe, soit il n'existe pas. Voilà une réponse honnête à une question directe. Il est toutefois possible qu'un degré de risque soit acceptable, il est possible que le risque zéro n'existe pas, mais une évaluation réaliste de cette dimension suivie du choix d'assurer ou non fait partie de votre stratégie financière d'entreprise. C'est à vous de faire le choix. À mon avis, la sélection d'une équipe, le travail en commun et des objectifs partagés sont le meilleur moyen d'éviter de poser des questions pour lesquelles vous n'êtes jamais sûr d'obtenir des réponses exactes. Un excès de précautions vous interdirait de lancer le moindre projet.

**MICHEL YARHI:** Comment gérez-vous le type de contraintes où existe le problème des coûts, quand il est moins cher pour votre entreprise d'acheter les services d'un fournisseur bien que cela puisse présenter un risque de sécurité plus important ou de qualité réduite ? Cela donne-t-il lieu à des discussions avec le service des achats ou bien êtes-vous indépendants l'un de l'autre ?

**PATRICK SMITH:** Mon expérience de cette situation m'a appris qu'il ne faut pas payer à l'avance. Vous créez votre propre risque. Si vous payez alors que vous en êtes encore au stade de la conception, vous allez faire une lourde erreur. Nous avons ainsi mis sur pied un système de paiements décalés qui fait tout pour inciter les fournisseurs à satisfaire notre demande.

**UN AUTRE MOYEN EST DE RESPONSABILISER LES CLIENTS PAR RAPPORT À LEURS DONNÉES**

**PASCAL LOINTIER**

**FABRIZIO SECHI:** Nous nous trouvons dans une situation étrange car nous sommes fournisseurs de technologie et nous achetons beaucoup de services informatiques. Nous travaillons en partenariat avec les fournisseurs, qui savent que nous avons les mêmes objectifs qu'eux. Mais je serais curieux de connaître votre opinion sur les audits indépendants et sur les certifications de type BS. Cela nous revient cher et je ne suis pas sûr que les experts en informatique soient d'accord sur ce point. Est- il est important pour vous qu'un fournisseur de technologie soit certifié?

**MICHEL YARHI:** Il est très important pour nous de vérifier la qualité à chaque étape lorsque nous faisons appel à des fournisseurs extérieurs. Les conséquences d'une erreur sont toujours plus

## IL FAUT QU'EXISTE UN BESOIN DE CONVERGENCE TRÈS FORT

**GILBERT FLEPP**

importantes pour la banque que pour le fournisseur lui-même et le niveau d'assurance de ce dernier est moins élevé que le risque que nous prenons en externalisant le service. C'est pourquoi nous sommes obligés de vérifier la qualité du produit et nous n'utilisons un intervenant extérieur que lorsque nous sommes absolument sûrs qu'il présente les meilleurs gages de sérieux.

**ANDY BULGIN:** Je crois, Michel, que la question est de savoir si vous évaluez la qualité sur la base de la certification ? Si vous faisiez appel aux services de Fabrizio, diriez-vous qu'en raison de sa certification, vous achèteriez ses services sans autre forme de vérification ? Parce que si ce n'est pas le cas, on peut mettre en doute la valeur de cette certification.

**MICHEL YARHI:** Eh bien, il est probable qu'avec la certification... Nous savons tous qu'être certifié, prenons la norme ISO comme exemple, ne signifie pas grand-chose. Cela veut simplement dire que vous savez faire quelque chose en un temps donné. Mais si vos critères de qualité sont exécrables...

**ANDY BULGIN:** Je crois que ceci est très intéressant. Voulez-vous dire qu'il s'agit d'un minimum absolu que tout le monde exigera ? Et que sans ce minimum, personne ne vous prendra au sérieux, même si l'on sait que ces critères ne signifient rien ? Parce que dans un contexte pareil, on peut se demander si cela vaut vraiment la peine d'être certifié.

**MICHEL YARHI:** Autre chose ? Nous devons poursuivre car il nous reste encore trois autres questions à traiter. La création d'une culture de la sécurité . Nous en avons déjà un peu parlé, mais peut-être souhaitez-vous ajouter quelque chose ?

**MARTIN LESSER:** Je voudrais évoquer un petit problème entre le marketing et la sécurité informatique. En Allemagne, par exemple, l'Office fédéral de sécurité informatique a recommandé, il y a quelques années, que tous les utilisateurs désactivent Java Script sur leur navigateur Internet. Mais si un utilisateur faisait cela aujourd'hui, la plupart des pages Internet, surtout celles des grandes sociétés, seraient inaccessibles. Nous devons donc au dilemme suivant : suivre les recommandations de sécurité informatique ou celles du marketing. Jusqu'à présent, c'est le marketing qui a remporté cette bataille mais il me semble que les informaticiens vont avoir gain de cause à l'avenir en raison de la croissance des risques.

**MICHEL YARHI:** Avez-vous rencontré ce problème ? Comment gérez-vous cela en tant qu'entreprise, chez Ace?

**GILBERT FLEPP:** Eh bien, je pensais justement à un exemple intéressant : nous avons acquis une société de télécommunications qui a souhaité démontrer à ses clients la supériorité de ses services en leur offrant un CD-ROM contenant toutes sortes de services supplémentaires. Hélas, les 30 000 CD-ROM produits contenaient un virus et ils ont dû être rappelés. Ce qui touche à deux des questions évoquées, la précédente, et celle relative au conflit entre marketing et sécurité.

**MICHEL YARHI:** Autre chose?

**PASCAL LOINTIER:** En ce qui concerne la France, nous recommandons la mise en place de charte de bonne conduite pour les utilisateurs. Cela nous semble être une bonne manière de convaincre les gens et si un litige d'ordre juridique survient, vous pouvez vous appuyer sur ce document pour prouver que vous avez informé les utilisateurs d'Internet sur leurs droits et leurs devoirs. Un autre moyen est de responsabiliser les clients par rapport à leurs données et de leur sortir de l'idée qu'il y forcément a un spécialiste, quelque part, qui peut restaurer leurs données et leurs mots de passe comme par magie.

**ANDY BULGIN:** Ne croyez-vous pas, plus généralement, que nous sommes atteints du syndrome des mots de passe ? L'un de mes amis a tellement de mots de passe qu'il a dû les noter par écrit, ce qui est exactement l'inverse du but recherché. Nous parlons de protection des informations, mais nous en utilisons une telle quantité qu'il faut que quelqu'un puisse en contrôler le flux ; et il me semble que cela devient impossible. Cela aussi est un risque en soi.

**PATRICK SMITH:** C'est ce que l'on veut dire par culture de la sécurité. Le problème des mots de passe découle du fait qu'on ne peut pas espérer que tout le monde protègera correctement les siens et que l'on essaie en même temps de créer une culture basée sur la confiance. Alors cela devient très difficile.

**MARTIN LESSER:** Mais dans la vie courante, quand les gens travaillent ensemble dans un bureau, si quelque chose ne fonctionne pas, vous demandez à votre voisin de vous prêter son ordinateur et son mot de passe, non ? On vit en groupe, les gens se font confiance et ne voient aucune raison de ne pas donner leur mot de passe à un collègue, par exemple. Il est difficile d'empêcher cela.

**DANIËL JACOBS:** Mais vous n'allez pas donner le code de votre carte de crédit à votre collègue et lui demander d'aller chercher 50 € pour vous à la banque. Ça ne se fait pas. C'est juste une question de culture.

**MARTIN LESSER:** Oui, c'est une question de culture mais le personnel ne réagit pas comme ça dans le cadre du travail. Il y a une différence entre donner son code de carte de crédit à un collègue et lui donner un mot de passe ayant un rapport avec l'entreprise pour laquelle vous travaillez tous les deux.

**PATRICK SMITH:** Cela dépend de la manière dont ces choses sont transmises. Trop souvent, ce sont les inconvénients qui sont mis en avant. Pas les avantages, toujours les inconvénients. Et parfois même, les pénalités. Vous régentez alors en imposant des sanctions, pas en utilisant des arguments rationnels montrant les avantages ou le côté logique.

**GILBERT FLEPP:** Et afin d'améliorer cette culture, celle de la sécurité informatique, il faut qu'existe un besoin de convergence très fort entre les différents domaines de responsabilité d'une entreprise. Or cela prend du temps et c'est très dur à mettre en place.

**MICHEL YARHI:** En ce qui concerne votre carte de crédit, pour faire une comparaison, on peut penser que les collaborateurs au sein d'une même entreprise ont un but commun, celui de faire avancer leur société. Il arrive que vous donniez le code de votre carte de crédit à votre femme parce que vous êtes dans le même bateau et que c'est pour le bien de votre famille. C'est plutôt délicat, mais le problème est celui du degré de confiance que vous avez dans l'autre personne. Bien sûr, il y a une différence entre un collègue et un conjoint. Mais, au sein d'une famille ou d'une entreprise, on poursuit normalement le même but. Tout le problème est bien là : quand les choses tournent mal, il arrive que quelqu'un considère qu'il ne fait plus partie de la famille.

**MARTIN LESSER:** Ce problème disparaîtra à l'avenir car beaucoup d'entreprises remplaceront les mots de passe par les systèmes biométriques. Ce n'est qu'une question d'années avant que nous scannions les empreintes digitales.

**MICHEL YARHI:** Nous n'avons plus beaucoup de temps et il nous reste encore deux sujets à traiter. D'abord, la création d'un environnement opérationnel permettant de gérer et de réduire le risque. C'est facile car vous pratiquez tous ce genre de chose.

**JEAN-MICHEL PARIS:** En tant que risk managers, nous devrions peut-être remettre en question un certain nombre de points clés. Revenir à l'identification du risque initiale, à vos évaluations des risques et ensuite, s'il reste encore des problèmes à résoudre, se dire: "il faut que je traite cet aspect là parce que c'est la meilleure manière de réduire le risque". Lorsqu'il s'agit d'informatique, vous vous dites probablement la chose suivante: "J'ai besoin de développer un nouveau logiciel pour un service donné, mais je veux qu'il soit nettement séparé du reste de l'environnement opérationnel. J'ai donc besoin de procédures spéciales pour l'entrée en service. Il me faut donc deux équipes distinctes et je n'aurais pas de feu vert tant que nous ne serons pas sûrs de ceci et de cela, que tout n'aura pas été mis noir sur blanc, ..." Même si vous ne maîtrisez pas toutes les finesses d'une technologie, vous pouvez toujours avoir quelque chose à dire en tant que professionnel de la gestion des risques.

**MICHAEL ROSSI:** L'une des meilleures pratiques de travail qu'il m'ait été donné de voir, on en a déjà parlé ici même si beaucoup de mes clients ne s'y sont pas encore mis, c'est lorsque le gestionnaire de risques et le service informatique travaillent ensemble et unissent leurs compétences. L'équipe peut ainsi décider ensemble de l'utilisation optimale des sommes destinées au contrôle des pertes ou des risques et auprès de qui effectuer la couverture d'assurance. Il est impossible pour un gestionnaire d'assurer les risques sans l'aide du département informatique car il faut effectuer des audits de sécurité et remplir des questionnaires d'assurance. Mais il faut que la décision soit prise en commun et que l'on s'entende sur l'utilisation de la prime d'assurance. On devrait les consacrer à assurer les risque graves mais peu fréquents. Sans l'aide des informaticiens, le gestionnaire va ramer dans un océan d'ignorance. Le travail d'équipe, c'est pour moi la meilleure façon de procéder et il semble que c'est aussi votre optique. Mais il est intéressant de constater que beaucoup d'entreprises

**VOUS POUVEZ INVESTIR AUTANT D'ARGENT QUE VOUS VOUDREZ DANS LA GESTION DES RISQUES, LES SINISTRES NE DISPARAÎTRONT PAS POUR AUTANT**
**MICHAEL ROSSI**

n'agissent pas comme ça : le gestionnaire de risques essaie, seul, de déterminer ce qui doit être assuré sans aucune aide de ses collègues du service informatique. Les choses sont en train de s'arranger. Il y a encore cinq ans, les informaticiens dans beaucoup d'entreprises ne voulaient pas qu'on s'adresse à eux. Ils se considéraient comme indépendants du reste de l'entreprise et ne répondaient à aucune question touchant à la sécurité, même de la part des souscripteurs d'assurance, de crainte que quelqu'un n'exploite les failles du système. Les choses sont en train d'évoluer car, à mon avis, de plus en plus de gestionnaires de risques font leur entrée dans les services informatiques. Travaillons ensemble. Tout dépend du mode de communication avec les informaticiens. "Je ne cherche pas à surveiller votre travail, je veux plutôt travailler avec vous pour qu'ensemble, nous puissions mettre sur pied une

**C'EST VOTRE RÉACTION IMMÉDIATE QUI VA DÉCIDER DE VOTRE SURVIE. C'EST ELLE QUI PERMET DE SAUVEGARDER VOTRE RÉPUTATION**
**ANDY BULGIN**

stratégie qui serve notre entreprise." À mon avis, c'est ce qui marche le mieux.

**MICHEL YARHI:** Merci. Il nous reste un quart d'heure, juste assez de temps pour notre dernier sujet : la protection contre les menaces extérieures (virus et piratage) ou intérieures.

**PASCAL LOINTIER:** Puis-je commencer ? Tout d'abord, vous avez parlé des virus comme de la hantise principale des sociétés. Notre association de sécurité informatique conduit périodiquement une enquête au niveau national. Dans la dernière en date, les virus inspiraient beaucoup de craintes, mais les entreprises savent également que le danger pour leurs ordinateurs est modéré. Il y a donc une contradiction entre la peur des virus et le fait que ceux-ci sont loin de représenter le plus grand risque de perte potentielle. Ceci est peut-être dû au battage médiatique organisé par un magazine d'informatique, qui expliquait que la moindre lettre d'amour était forcément un virus déguisé. Or, même dans votre étude, les gens en ont toujours peur. Les virus ne se comportent pourtant plus comme dans le passé. Dans le temps, ils effaçaient simplement les données au hasard. De nos jours, ils ont plutôt tendance à ralentir le réseau ou à créer des dysfonctionnements, voire à mettre hors service des ordinateurs portables ou de bureau. Mais ils ne détruisent plus les données comme c'était le cas auparavant et comme cela pourrait se reproduire à l'avenir.

**MARTIN LESSER:** Le piratage a pris une dimension commerciale. Beaucoup de gens, dans le monde entier, mettent sur pied des botnets, ce qui signifie que des milliers d'ordinateurs sont placés sous le contrôle d'une seule personne et qu'ils peuvent être utilisés en réseau pour attaquer votre société. Vous aurez de sérieux problèmes si un botnet, c'est-à-dire 20 000 à 30 000 ordinateurs, attaquent soudainement votre réseau. À l'heure actuelle, on pense qu'environ 2 millions d'ordinateurs sont sous le contrôle de pirates. C'est le chiffre qui circule.

**MICHAEL ROSSI:** Je suis d'accord avec ce que vient de dire Martin et à mon avis, même si la majorité d'entre vous pense le contraire, peu importe le degré de protection ou de gestion des risques que vous mettez en place, le risque est toujours là. Vol de données, systèmes en panne… Et nous continuons à voir des sinistres, dont certains ne sont pas déclarés de manière spécifique ; il y a aussi les cas de cyber-extorsion, tout simplement parce que les gens sont réticents à déclarer publiquement avoir été victime d'un piratage. Nous avons connaissance de sinistres dus à des virus s'élevant à 10 ou 14 millions de dollars US. Il y a aussi des sinistres de 50 millions de dollars US dus à la destruction malveillante de données par les employés. Vous pouvez investir autant d'argent que vous voudrez dans la gestion des risques, les sinistres ne disparaîtront pas pour autant. Et pour moi, la vraie question, dans la mesure où les sinistres sont toujours possibles, c'est de savoir si oui ou non, il faut les assurer. Les avis sont très partagés. Il y en a qui disent non, si un sinistre de première partie survient, on n'assure que les pertes catastrophiques (50, 100 ou 150 millions). Mais ce n'est suffisant. En ce qui concerne la RC, "on est assuré parce qu'on a une garantie RC diffamation ou sinon une garantie pertes financières". Pour moi, les questions délicates sont de savoir qu'est-ce qui est assuré, qu'est-ce qui ne l'est pas ? Comment faire le départager ? Et si ce n'est pas couvert, le risque est-il suffisamment sérieux pour qu'il faille prendre une assurance ? Tout ce dont vous pouvez être sûr, c'est que le risque existe, quel que soit le degré de gestion.

**MICHEL YARHI:** Je dirais que pour une banque, l'assurance n'est pas un vrai problème. Si quelqu'un réussit une opération de phishing, si les codes d'accès de cartes de crédits sont piratés, ce n'est plus un problème d'assurance : cela devient un problème de confiance entre le client et la banque. Si la confiance disparaît, la banque peut fermer. Cela n'a rien à voir avec les questions d'assurance. Alors ce qui est le plus important pour nous, c'est d'éviter les attaques, et s'il y en a une, d'en limiter les conséquences.

**ANDY BULGIN:** Je pense en effet que votre deuxième argument est tout à fait valable. Si vous prenez un problème sous l'angle de la gestion du risque, c'est votre réaction immédiate qui va décider de votre survie. C'est elle qui permet de sauvegarder votre réputation. Il se peut que vous perdiez de l'argent et peut-être allez-vous en récupérer une partie grâce aux assureurs, mais c'est le moindre de vos problèmes. Préserver la réputation de votre banque, ou celle de notre entreprise de boissons, voilà ce qui va déterminer la survie de l'entreprise. Par ailleurs, nous parlons ici de la protection des données. Il me semble que beaucoup d'entreprises n'ont pas conscience du caractère très sensible des informations qu'ils détiennent. Le vol d'informations relatives au personnel est, par exemple, un gros problème aux États-Unis, avec l'usurpation d'identité et autre. Nombre de cadres n'ont aucune idée des implications ou du coût de ce genre de vol pour l'entreprise. C'est probablement sur cela que nous devons faire porter nos efforts : faire comprendre à nos collaborateurs ce qui risque d'arriver en cas de priatage d'informations de ce type. Le risque peut être bien plus qu'avec de simples données d'entreprise.