



INTERNATIONAL BUSINESS AND
PROFESSIONAL MAGAZINE OF THE YEAR

Strategic**RISK**



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 PROGRESSSM

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 Générale 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

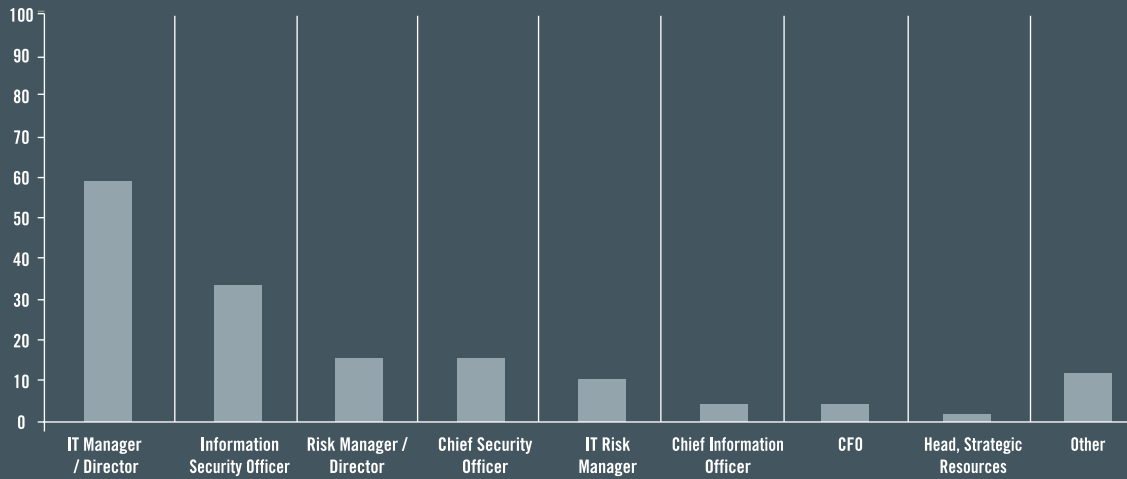


Michael Rossi
President, Insurance Law Group

For more information about ACE, please email euro.comms@ace-ina.com or visit www.aceeuropeangroup.com

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.

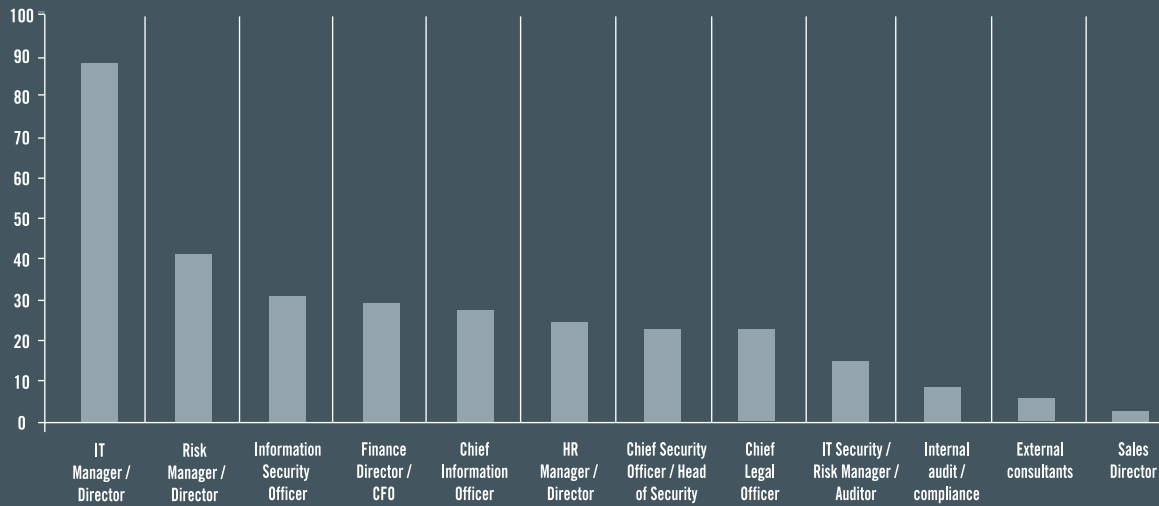
As for internal IT threats, human error tops the table, with employee theft or misuse of data a very close second. The risk of a departing employee taking information and misusing it is a particularly widespread concern.

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

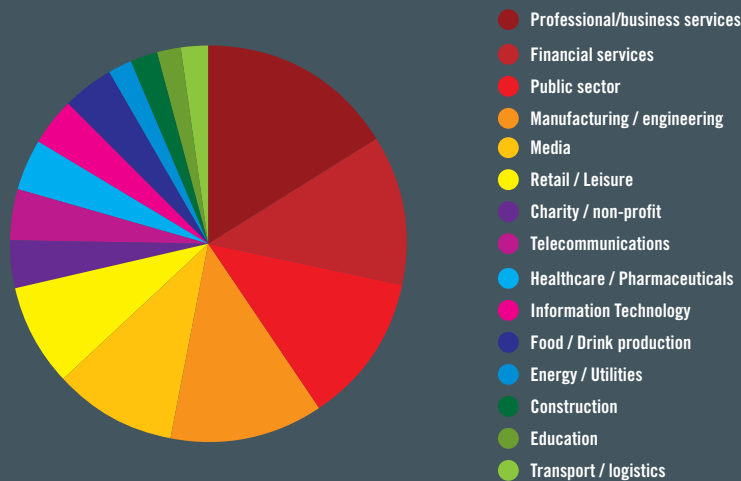
to their general commercial material damage and business interruption policies to include some cover for IT-related risks. Several respondents expressed a wish for more clarity, information and advice on this subject.

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

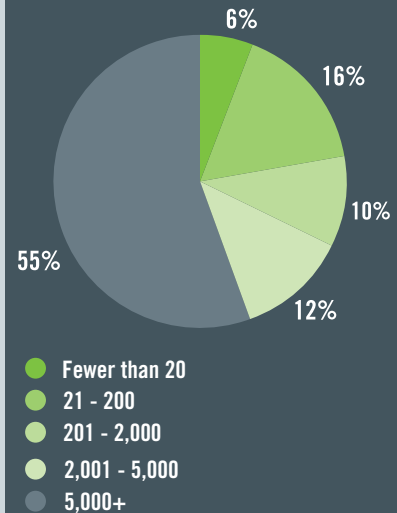


Respondents by Business Sector

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?

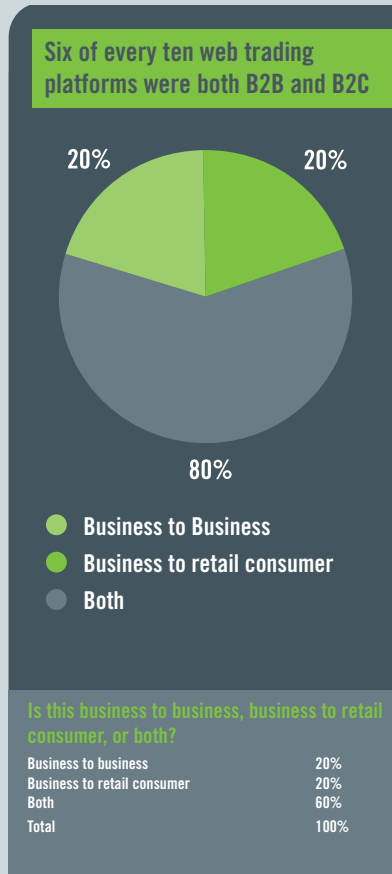
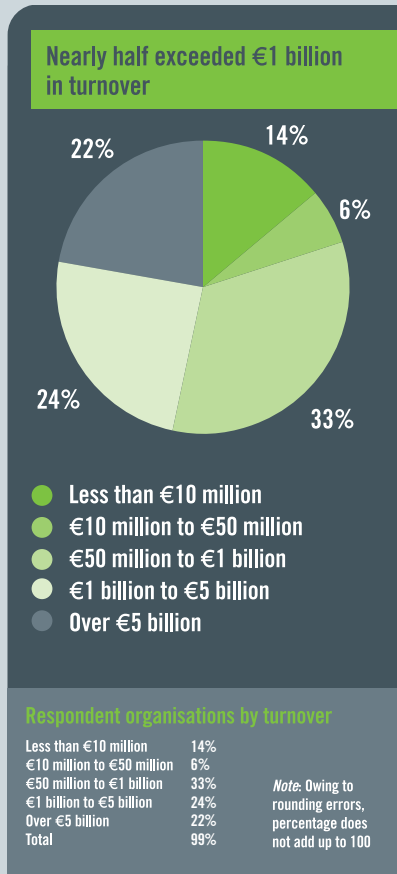
Yes	52%
No	48%
Total	100%

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



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



THE STAKES ARE RISING

JEAN-MICHEL PARIS

were the efforts to deal with it, but now we are being forced to deal with it in a very organised and structured way.

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,



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

DANIEL JACOBS

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.

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



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 balk 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



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

FABRIZIO SEECHE

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-built 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.

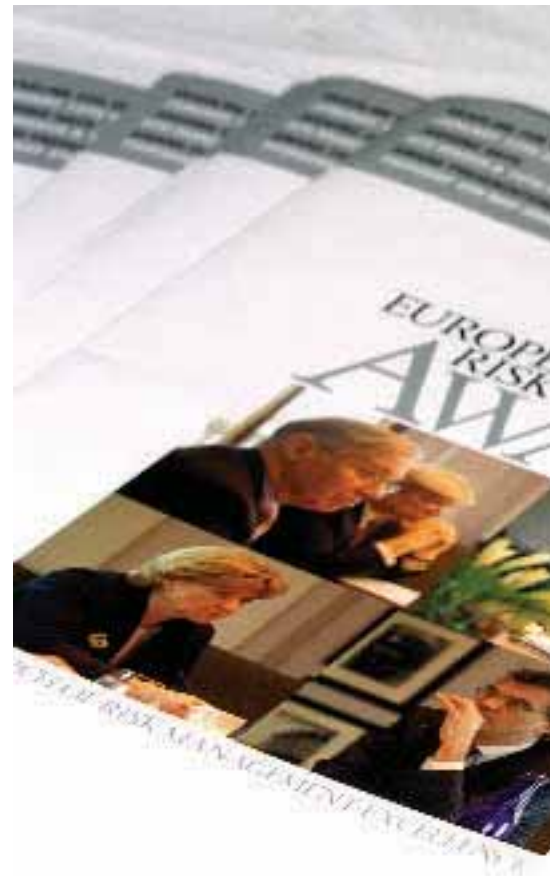
MARTIN LESSER: Yes, it's the culture, but the normal staff member does not think that way. It's a different matter giving his colleague his credit card, from giving him a password which is effective

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.