#5

# ACE EUROPEAN RISK BRIEFING 2012

IT and cyber risk

# RESPONDENT PROFILES

The research was carried out between 13 April and 3 May 2012. The sample comprised 606 European risk managers, CROs, CFOs, COOs and those responsible for buying insurance.

Interviews were conducted by telephone by Opinion Matters on behalf of ACE Europe. Respondents were chosen at random from a pre-selected database and were screened for eligibility. Respondents were not compensated for their participation and ACE was not identified as the research sponsor. Percentages have been rounded for ease of reading, and totals may therefore add up to more or less than 100%.

## Respondents by job title

| | |
|---|---|
| Chief risk officer | 27% |
| Chief financial officer | 25% |
| Chief operating officer | 24% |
| European risk manager | 23% |

## Respondents by size

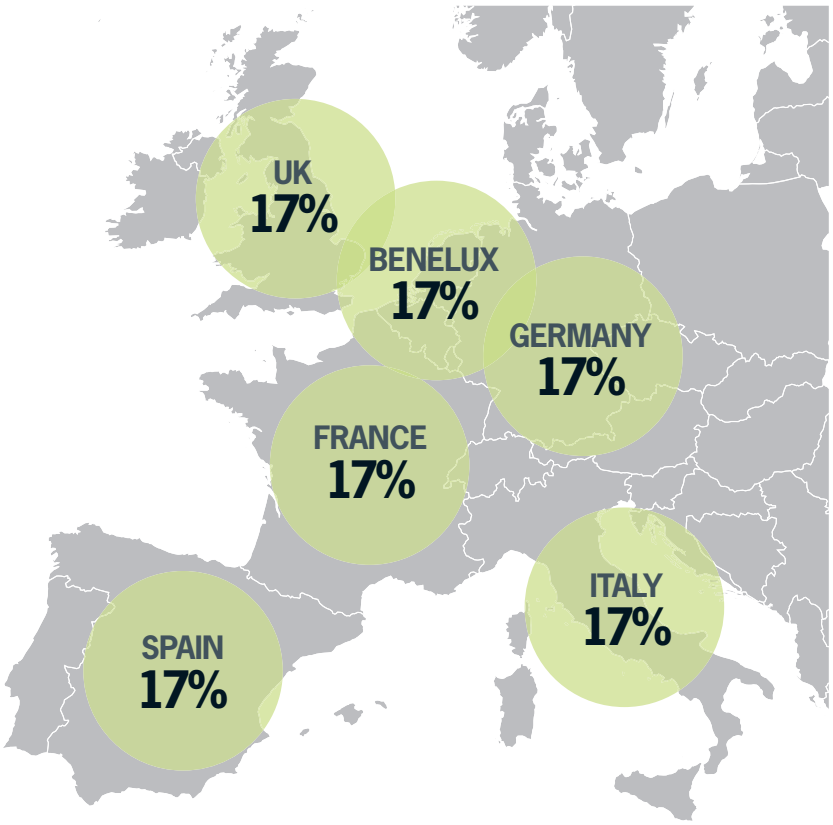


| | |
|---|---|
| £500–700m turnover | 51% |
| Over £700m turnover | 49% |

## Respondents by company sector

| | |
|---|---|
| Architecture, engineering and building | 5% |
| Retail, catering and leisure | 5% |
| Manufacturing and utilities | 6% |
| Sales, media and marketing | 6% |
| Legal | 7% |
| Education | 7% |
| Professional services | 7% |
| Travel | 8% |
| Arts and culture | 9% |
| Healthcare | 9% |
| IT & telecoms | 9% |
| HR | 10% |
| Finance | 12% |

## Respondents by country



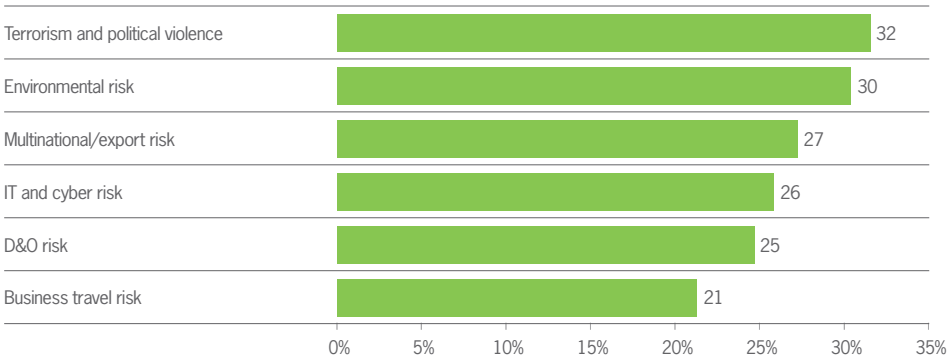
# IT AND CYBER RISK

Almost every company today depends on communication, service or commerce delivered over the internet and other information networks. The scale of this reliance seems to be steadily growing. Companies store ever-increasing quantities of sensitive personal and commercial information online, while developments such as cloud computing mean that their data is often no longer stored within the company's own networks, but remotely.

Technology has been a powerful enabler of economic growth, helping small companies to become international and large companies to go global. But at the same time, it has created a new category of risks that can be severely damaging, yet are often poorly understood.

Cyber and IT risks are extremely varied. They range from the effects of mundane human errors, such as leaving a laptop on a train, right through to large-scale hacktivism, cyber-espionage or denial-of-service attacks. They can also be very costly and widespread. According to one estimate, the cost of cybercrime globally in 2011 reached US $388bn, (around €300bn) with an individual falling victim to some form of online crime every 19 seconds.[1] Any of these can have a wide range of business consequences including reputational damage, regulatory fines and the financial losses caused by business interruption.

**Which of the following risk areas are most relevant/ important to your company today?**




Overall, in comparison with other risk categories researched by ACE, European companies rank IT and cyber risk relatively low on their list of priorities. It is seen as less important than terrorism, environmental and multinational risk, for example. However, it is ranked as the second most important emerging risk by larger companies (cited by 29%) suggesting that multinationals and other businesses with turnover of over €800m are waking up to the risks.

[1] Norton Cybercrime Report, 2011

**"THE COST OF CYBERCRIME GLOBALLY IN 2011 REACHED US $388 BN, WITH AN INDIVIDUAL FALLING VICTIM TO SOME FORM OF ONLINE CRIME EVERY 19 SECONDS"**

> “JUST 48% OF RESPONDENTS SAY THAT THEY ARE PREPARED TO MANAGE IT AND CYBER RISK”

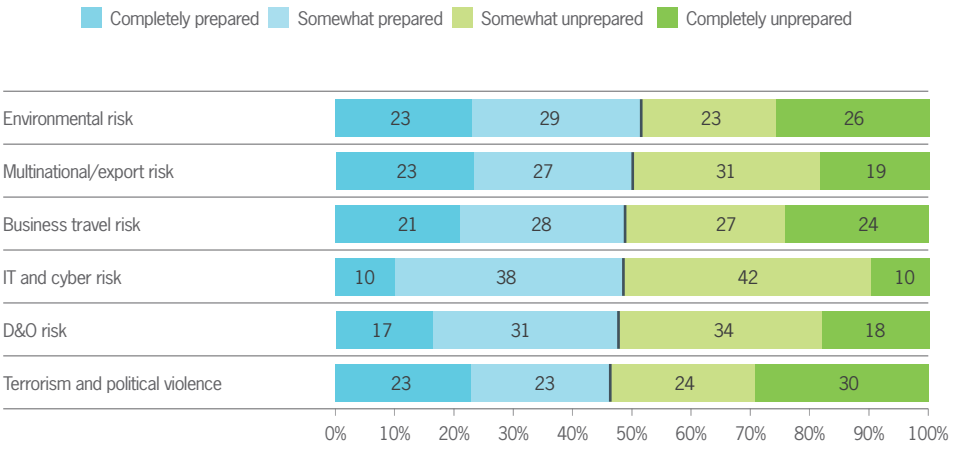
## Evolving phenomenon

In some respects, it seems surprising that mid-sized companies do not consider these risks to be more of a threat. The pervasive reach of information technology, and the critical role that it plays in business models, mean that any major IT or cyber-risk event can quickly have severe consequences. In addition, it is a category of risk which is evolving very quickly and is increasingly the subject of media headlines.

One of the reasons cyber risk does not top the list of emerging risks for European companies overall may be that it is not well understood. As a relatively new phenomenon, it is inherently less familiar than some other risk types. It is certainly a category of risk for which few companies feel well prepared. Just 48% of respondents say that they are either completely or somewhat prepared to manage IT and cyber risk.

Nonetheless, some 42% of companies believe the level of IT and cyber risk their company experiences will increase over the next five years. As economic activity shifts from the physical to the virtual world, the range of cyber and IT threats continues to broaden. Moreover, it can be much easier for would-be cyber-attackers to inflict damage on corporates through virtual rather than physical means. In theory, a single hacker can now potentially disrupt an entire computer network from anywhere in the world, while a computer virus can inflict untold reputational and financial damage.

**How would you rate your company's level of preparedness for each of the following risk areas?**



> “IT SEEMS INCONSISTENT THAT COMPANIES DO NOT CONSIDER PUBLIC LEAKS OF SENSITIVE INFORMATION A GREATER WORRY”

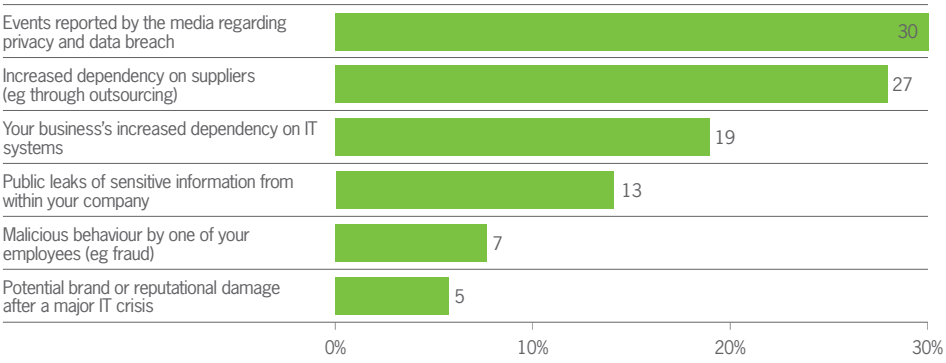
## Risk events

So what would cause European businesses to become more concerned about cyber risks? Two factors emerge as dominant from ACE research. Increased media attention of privacy and data breaches ranks in top place. European companies appear to be well aware of the risk of a data leak ending up in the newspapers in today's more intense news environment. Increased reliance on external suppliers is the second most popular answer, as supply chains continue to grow more complex and outsourcing for a wide range of functions becomes embedded within many companies' operations. Increased dependency on IT systems generally ranks notably in third place.

Some risk events will involve a combination of these factors. The risks associated with outsourcing can be a particular worry because it is more difficult for companies to ensure that data handed over to the provider is adequately protected. The purchaser of an outsourced service may have extremely robust IT security controls but it does not follow that a company to which it hands over precious data has the same level of protection.

This fact was clearly demonstrated in March 2011, when the marketing services company Epsilon revealed that hackers had compromised its IT systems and stolen customer details belonging to clients including JP Morgan, Chase and Best Buy. Estimates for the potential losses from the event, which include forensic audits, fines, litigation, and lost business, may be as high as US $4bn (around €3.1bn).[2]

**What type of internal incident would make your organisation more concerned about cyber risks?**




Other incidents, such as public leaks of sensitive information or malicious behaviour by employees, come further down the priority list. It seems inconsistent that companies do not consider public leaks of sensitive information a greater worry, given their sensitivity to media reporting of data breaches. The rise of social media, Twitter and other channels means that information can now be disseminated around the world in a matter of seconds. In addition, these are channels over which no company can exert much control. Good risk management practice is therefore to ensure that sensitive information is carefully restricted within the company in the first place.

[2] Infosec Island, 'Ten most expensive network attacks in history', 18 August 2011

> “MOST APPEAR VULNERABLE TO AN EXTREMELY BROAD RANGE OF CYBER RISKS RELATED TO SYSTEMS FAILURES, AS WELL AS MALICIOUS ATTACKS”

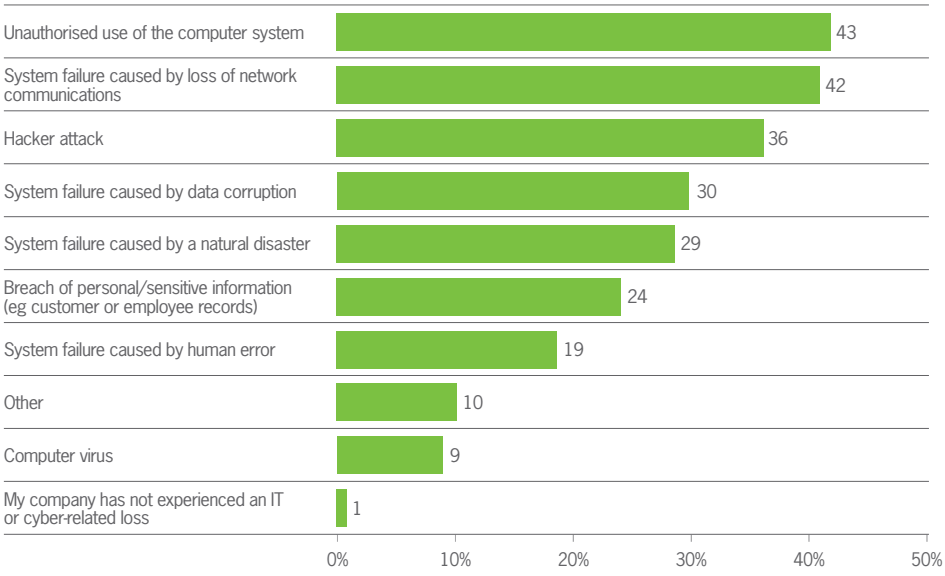
## Malice or mishap

Although IT and cyber risks are extremely diverse, they can be broadly divided into two categories: deliberate, malicious events, such as hacking, unauthorised use, cyber-espionage or computer viruses; and those that relate to systems failures, which may be caused by unintentional human error or by an external event, such as a power cut or natural disaster.

Among respondents to our survey, only a tiny minority of European companies report no problems with cyber or IT risk. Just 1% say that they have not experienced an IT or cyber-related loss over the past five years, which illustrates just how prevalent these issues are. Moreover, there is no single category to which European companies typically fall victim. Most appear vulnerable to an extremely broad range of cyber risks related to systems failures as well as deliberate or malicious attacks.

The most common type of loss relates to the unauthorised use of computer systems. This could cover a variety of situations, including the theft of personal or commercial data, or espionage by internal or external agents. In general, it is more likely that theft of data will be carried out by internal rather than external agents,[3] so this highlights the importance of strong risk and controls frameworks and encryption processes. In addition, continuing economic uncertainty and the potential loss of jobs in many developed markets mean that data theft could become more commonplace as disgruntled employees (or former employees) seek to exploit a company's digital assets for personal gain.

**Which of the following exposures have generated a loss for your company in the last five years?**




Losses associated with a systems failure generally rank in second place, but incidents involving hackers are not far behind. 36% of European companies say they have experienced a loss as a result of hacking over the past five years. Recently, a new term – hacktivism – has entered the corporate lexicon to describe a particular type of hacking carried out to make a political or protest point. In 2011, the security firm HBGary became a prominent victim after it claimed to have information about the identities of a group of hacktivists, known as Anonymous. In revenge, Anonymous hacked into HBGary's networks, brought down their phone system and even took over their CEO's Twitter account and published his social security number online.[4]

[3] 2011 Data Breach Investigations Report produced for Verizon

[4] World Economic Forum 2012, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

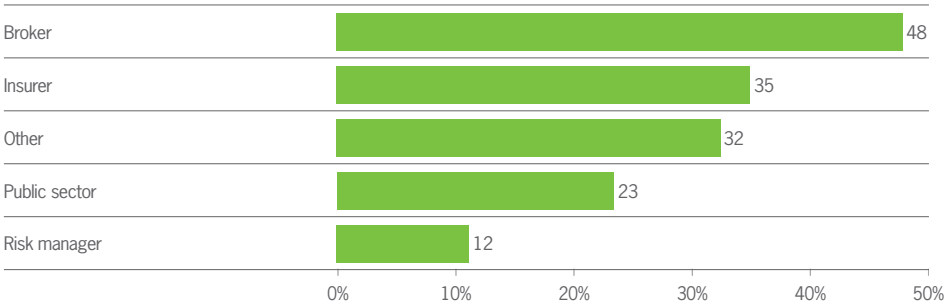
## Cyber insurance: an evolving market

There are few risk categories that are as fast moving as cyber and IT risk. The range of threats that companies face is extremely broad, and is constantly evolving as new technologies and techniques emerge.

An added dimension to the risk environment is now being provided by regulators, who are also paying close attention to cyber risks. The proposed Data Directive in the European Union could mean that companies are liable to a fine equivalent to 2% of their worldwide revenues if it can be demonstrated that they have not done enough to protect sensitive data.

Given the dynamic nature of cyber risk and a self-confessed lack of understanding on the part of many European companies in our study, the importance of receiving a constant flow of information about the changing environment has never been greater. Numerous sources for this information exist but risk managers trail at the bottom of the list, underlining the lack of confidence that many companies have in their own ability to monitor and analyse this particular area of risk.

**For each of the six risk areas we have discussed today, who do you rely on for information on the changing risk environment?**




Among our respondents, brokers are the most popular source of insight by some margin. Yet ACE's own experience is that not all brokers are actively engaged on cyber risk issues. At a briefing for over 100 brokers in London in summer 2012, over half of UK insurance brokers (58%) said they do currently discuss cyber risk with their clients. Insurers rank in second place as a source of insight. Together, these findings emphasise clients' reliance on the insurance industry as a partner for monitoring and assessing the changing risk environment. They also highlight the importance of broker and insurer working together to develop new risk solutions for this evolving risk.

> "FINDINGS HIGHLIGHT THE IMPORTANCE OF BROKER AND INSURER WORKING TOGETHER TO DEVELOP NEW RISK SOLUTIONS FOR THIS EVOLVING RISK"

> "BUSINESSES NEED TO EMBED A RISK CULTURE THAT ENSURES THAT THERE IS AN ENTERPRISE-WIDE FOCUS"

## Lack of understanding

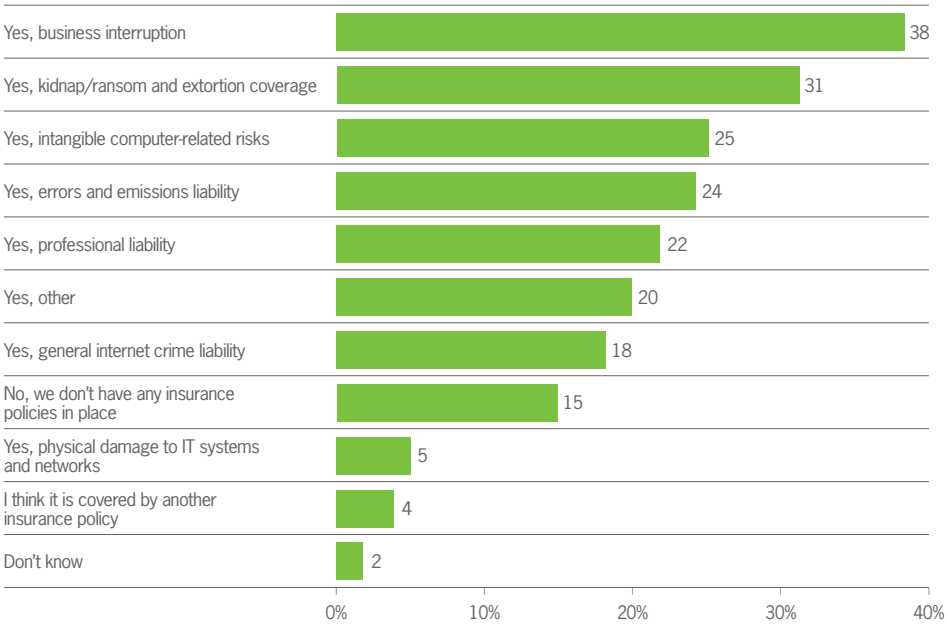
As with several other emerging risk categories discussed in this research series, there appears to be a low level of consistency among European companies in respect of insurance purchasing behaviour. In particular, a lack of detailed understanding about when cyber risks are included in or excluded from other insurance policies is apparent.

Over one third of European companies (38%) believe that they have specific insurance for IT risks under their business interruption policies, while 31% say that they are covered for some risks under kidnap, ransom and extortion coverage. However, in practice, many traditional commercial property and casualty policies fall short of the cover needed for comprehensive protection against the risks associated with first-party risks and potential third-party liabilities.

Approximately 20% of European companies say either that they do not have specific insurance policies to cover these risks, or they are unsure about whether they are covered or not. One recent very high profile and costly case of data breach resulted in a court case to determine whether or not these risks were covered by a company's insurance policies, highlighting the importance of businesses checking that they have adequate cover in place.

The specialist cyber insurance market is a relatively young, although fast-growing sector. The products available for both first-party and increasingly third-party risks too are continually evolving and improving.

**Do you have insurance in place specifically to cover IT risks?**




Ultimately, however, insurance should be seen as just one part of an appropriate approach to risk management. Many companies still need to get to grips better with monitoring and reporting on their exposures to cyber and IT risk. Installing security systems that will give them protection against a range of potential attacks or problems should be a first priority. Businesses would also do well to focus on how and where their data is stored, and put protective measures in place to ensure that security is not at risk of being breached in the first place.

Perhaps most importantly, they need to embed a risk culture that elevates these important risks out of the IT function and ensures that there is an enterprise-wide focus, and a clear risk management framework, on how to manage information security.