Special Report

Cyber risks

CYBER RISKS

THE GROWTH OF THE INTERNET HAS CREATED A NEW business and personal environment. Communication – and reaction – is almost instantaneous. Programs allow customers' details to be stored immediately. Social networking allows businesses to reach a far wider audience than their existing business base and potential readers of advertisements.

This new environment has evolved very quickly, and it is still developing. Unfortunately, so are the associated threats and risks.

The most common risk businesses face is data theft. As internet banking and e-trading have become accepted activities, corporations have had to protect the information their customers entrust to them. But data breaches have become common, raising questions over website security. European countries have developed their own rules and penalties but inevitably the European Commission is wading in with a proposed new regime across member states.

Far less easy for legislators to tackle is the issue of social networking and how freely employees can express themselves as regards their employer and colleagues. Different countries take different views. In the USA, for example, it seems that the right of employees to criticise their employers in some cases is defended more rigorously than it is in some European countries.

But other, possibly more dangerous, threats are emerging. Cyber espionage – theft of confidential corporate information – appears to be increasing. The use of viruses to attack the systems that companies use to run their businesses may also be growing.

The frightening aspect of such activity is that it may not be easily detectible, and associated losses could be huge. The theft of a strategic plan or R&D results – or tampering with systems that run an integral part of production – could annihilate profits.

In a virtual world, companies have to accept that any breach of IT security is likely to have a major impact on their reputation. In the future, it may be that those companies that can demonstrate superlative security are the winners.

Contents

[CYBER RISKS]

SPONSORED BY

CHARTIS

This special report has been produced with input from Chartis:
Shanil Williams, VP financial lines shanil.williams@chartisinsurance.com
Steve Bonnington, VP financial lines steve.bonnington@chartisinsurance.com

CYBER ATTACKS

Worms and virtual warfare

The Stuxnet virus that hit computers in Iran were the first time many of us had heard of cyber warfare. But experts warn such attacks will be a key challenge for companies and organisations in the 21st century

WHILE ISSUES AROUND DATA security and employees' social networking tend to be the stories that hit the headlines, there are other cyber risks that potentially pose graver threats.

Global Risks 2012, the seventh edition of the World Economic Forum's (WEF) annual risk report, published in January, talks at some length about "the dark side of connectivity". It says: "The impacts of crime, terrorism and war in the virtual world have yet to equal that of the physical world, but there is fear that this could change."

The Stuxnet worm could be a wake-up call: it targeted the Siemens equipment used in nuclear facilities in Iran. "While evidence of the impacts of Stuxnet is questionable … its broader significance lies in suggesting what is possible," says the WEF. And it is not only government operations that may be targeted.

The WEF cites the case last year of four people arrested in the Philippines over the hacking into of US telecommunications companies' systems, resulting in losses of $2m (€1.5m) for AT&T alone, funds moved to the accounts of terrorist financiers.

It warns too that "subversion" can severely damage reputations and undermine trust. "For example, in 2011 the US technology security firm HBGary Federal – whose clients include the US government and McAfee – claimed to have information on the identities of a notorious group of activist hackers, or 'hacktivists', known as Anonymous. In response, Anonymous infiltrated HBGary's servers, libelled them on their own website, published 40,000 of the company's private emails, took down their phone system, took over their chief executive officer's Twitter account and posted his social security number online."

A white paper published in January by US law firm Edwards Wildman, *Everyone's*

'Potentially, the consequential business loss for companies both in the short term and from loss of future revenues dwarfs the cost of all the other cyber risks' **Henry Harrison** Detica

DATA PROTECTION

Keeping it confidential

The growing number of data protection breaches has prompted a European Commission move to harmonise regulations. But not everyone thinks they go far enough, or that they will make compliance easier

DATA SECURITY REMAINS A RISK for businesses in terms of protecting the personal information that they hold on individuals as well as confidential corporate data. "There appears to have been a huge increase in criminals using the internet to steal information and, despite companies' endeavours to take preventive measures, incidents still keep occurring," says risk management consultant Chris Luck.

"This suggests that some businesses are not doing as much as they could in checking for flaws in their systems. Hackers seem to be developing their techniques faster than the security solutions designed to combat them."

The European Commission is poised to step in with proposals to end continuing data breaches and a hotchpotch of regulation. On 25 January, it announced plans for common rules across member states, saying this would remove fragmentation and administrative burdens, "leading to savings for businesses of around €2.3bn a year".

The proposed new rules have met with a mixed reception from security experts. Interoute security services product manager Jeff Finch says: "There is some good news. The collation of harmonised data protection rules across 27 countries will without a doubt save organisations from a headache. Piecing together differing national data protection laws will have felt like one massive patchwork task, especially as cloud computing placed question marks over the location of data.

"The next step is to look for harmonisation with laws in other countries like the USA, where the Patriot Act enables authorities to search telephone, e-mail, and financial records without a court order. Thus, understanding where data resides and in whose data centre will continue to be a crucial part of corporate governance."

Informatica senior vice-president of global sales strategy Charles Race suggests businesses will need to re-evaluate their efforts to prevent data breaches. "Already the subject of stringent regulation and the risk of hefty fines from the UK Financial Services Authority, following these new standards the financial services industry in particular will be feeling the heat to make doubly sure that data security measures are up to scratch," he says.

nightmare – privacy and data breach risks, states: "Another type of cyber risk has become increasingly prominent: cyber attacks that are directed not at acquiring information, but rather at causing significant physical effects or business disruption, including destruction or disruption of computer control systems, and the industrial systems and equipment on which the operations of industrial entities and public utilities depend."

Edwards Wildman quotes former US deputy defence secretary Robert Gates: "In the twenty-first century, bits and bytes are as threatening as bullets and bombs."

Cyber espionage – theft of commercially sensitive information – is increasing too. At *StrategicRISK*'s 100 risk retreat in November, Detica technical director Henry Harrison said incidents had been reported by the chemical, oil and gas industries and other businesses. Most occurrences are either not detected or not reported, however. "Potentially, the consequential business loss for companies both in the short term and from loss of future revenues dwarfs the cost of all the other cyber risks," he said.

PricewaterhouseCoopers cyber and information security practice director William Beer says: "Cyber security is not just an IT issue. All public and private sector organisations need to transform their mindset. Leaders see cyber as a technical issue and fail to appreciate the business impact of an attack.

"Recent attacks have shown incredible resourcefulness and ability on the part of the criminals, and even the most cyber-savvy organisations have found themselves exposed and ill-prepared to manage the effects." SR

KEY QUESTIONS

- What steps can be taken to improve the sharing of information and build safeguards to reduce cyber threats?
- What incentives will mobilise businesses and the public sector to invest in the resilience of information infrastructures?
- How do we reconcile the benefits of innovation through open source software with the risk that individuals might manipulate code for malicious purposes?

Source: Global Risks 2012, World Economic Forum

Imperva director of security strategy Rob Rachwald considers the new EU privacy law to be a good step forward for individuals' privacy. "However, the proposal doesn't do enough to protect data," he says. "Since it mainly proposes fines, it will not help keep EU citizen data safe from hackers or insiders. Rather, the EU should put in place fines coupled with a more prescriptive approach, identifying specific actions firms should take to protect data."

Varonis Systems director of strategy David Gibson believes the migration to the new rules may be a complex process for some multinationals – and firms pushing into new countries. But he welcomed the news that companies with more than 250 staff will be required to appoint a data protection officer. "The appointment of a data protection officer will help focus the attention of many more companies on what has become a major issue for everyone in this digital age ," he says. SR

WHAT BRUSSELS PROPOSES

- A single set of rules on data protection removing unnecessary administration, such as notification requirements.
- Increased responsibility and accountability for those processing personal data.
- Organisations only having to deal with a single national data protection authority.
- People having easier access to their own data, being able to transfer personal data from one service provider to another more easily and delete their data if there are no legitimate grounds for retaining it.
- Application of EU rules if personal data is handled abroad by companies that are active in the EU market.
- Strengthening of national data protection authorities with the power to impose fines of up to €1m or 2% of global annual turnover for data protection breaches.
- A new directive applying general data protection principles and rules for police and judicial co-operation.

WEB 2.0

Anti-social media

The boom in the use of sites such as Facebook and Twitter has created opportunities for businesses – but they also have to beware what their employees might be saying about them

THE USE OF SOCIAL MEDIA SUCH as Facebook, LinkedIn and Twitter is a prime example of the risk versus opportunity conundrum. Companies have much to gain from embracing the opportunities provided to create and consolidate an audience of loyal followers. But their efforts may be undermined – inadvertently or deliberately – by the postings of their employees.

In a study by law firm DLA Piper, *Knowing your tweet from your trend*, partner Kate Hodgkiss says the next few years are likely to see major growth in the use of social media in the workplace, whether as a tool for organisations to communicate with a geographically diverse workforce, for training, or to let teams collaborate and share ideas.

"Whether you're a regular tweeter or new to the game, a Facebook aficionado or a beginner, there is no mistaking that Twitter, Facebook and LinkedIn have had a major impact on the way we interact and communicate. Unfortunately, the impact is not always positive," she says. "Employee use of social media, inside and outside the workplace, can expose employers to serious legal liabilities. Social media presents employers with some new problems, a new platform for existing problems and potential to magnify common business risks."

DLA Piper's study reveals that use of social media is landing employees in trouble:

- 21% of employers have taken disciplinary proceedings because of information an employee has posted on a social media site about another individual;
- 25% of employers have taken disciplinary proceedings because of information an employee has displayed about their activities at work;
- 31% of employers have taken disciplinary proceedings because of information an employee has posted about the organisation; and
- 30% of employers have taken disciplinary proceedings because of the level of an employee's social media use at work.

Commenting in *StrategicRISK*'s Amrae dailies, GDF Suez deputy chief risk officer, and vice-president of Ferma, Michel Dennery warns: "Social networking offers many opportunities for discussion among 'friends' who are mostly just online acquaintances. The tone is open, uninhibited, mocking and jokey. They believe themselves to be having a private conversation.

"However, these chats get picked up, forwarded to other friends and rumours develop independently of the original source. Control disappears. To expose to just anyone disparaging comments about the business or its management, when these should remain within the private domain, is a liability."

Lou Dubois on US website Inc.com says: "Whether it's in the hiring and recruitment process or when an employee is legally employed, setting a clear and specific standard for social media usage and guidance is a requirement. Defining what your employees can and cannot do, both in the workplace and at home, needs to be spelled out. If you fire an employee for something they've said on Facebook or on another social network, that needs to be spelled out in your own company's policy or you could be subject to a wrongful termination suit."

At October's Ferma Forum in a session called "The risks of the virtual world", Bureau Européen d'Information Commerciale secretary general Laurent Delhalle recommended that companies follow the example of an enlightened few that have already written guidelines or a charter for employees on using social networks. "This would constitute protection not just for the company but also the employee concerned, who might otherwise face an action for breach of confidentiality," he said.

DLA Piper suggests introducing or reviewing confidential information provisions and post termination restrictions in employment contracts on the use of social media, and using a social media policy to emphasise the ban on disclosure of confidential information and ownership of business contacts. Requiring employees to adopt 'closed' privacy settings on sites such as LinkedIn and stepping up monitoring during and after termination of employment to detect leaks of confidential information and misuse of contacts are further strategies.

But social media is not all negative. On Mashable Business's website, Levick Strategic Communications senior digital strategist Patrick Kerley says companies that have established a strong social media presence in "peace time" can use this to refute damaging allegations and even dominate search engines so that they communicate their side of the story first. **SR**

'Social media presents employers with some new problems, a new platform for existing problems and potential to magnify common business risks' **Kate Hodgkiss** DLA Piper

FACTS AND FIGURES

Top five risks of social media in the workplace:

1. HR policies and practices not keeping pace with technology
2. Bullying and harassment
3. Discrimination
4. Disclosure of confidential information
5. Damage to reputation and brand

Source: DLA Piper

Defamation is becoming a huge issue on social media sites as lawsuits for this particular offence are rising dramatically. In Canada and the USA, 15% of all web 2.0 rulings were on defamation cases. In France, it's 49% and in Quebec it's more than 10%.

Source: US PhysOrg.com