StrategicRISK
www.strategic-risk.eu
[November 2011]

Data security

Protecting private data from prying eyes poses some serious risk management questions. Here are the answers

property, liability, public liability, excess casualty, directors, officers, leisure industry, airlines, travel agents, hotels, resorts, restaurants, bistros, cargo, containers, harbors, cranes, accident and health, life insurance, reinsurance, marine, charter vessels, commercial hull, mega yachts, pleasure boats, whole life, term life, group life, disability, construction, skyscrapers, museums, public parks, offices, hospitals, agriculture, excess liability, medical malpractice, political risk, homeowners, automotive, fleet, 18-wheelers, vans, hybrids, motorcycles, scooters, school buses, estate, surety, products, damage, theft, landlords, lessees, retail, shopping malls, product liability, identity theft, data theft, data recovery, power stations, gas stations, refineries, drill islands, pipelines, natural gas, hydrogen, tankers, carbon waste, pollution, storage tanks, football clubs, cricket clubs, country clubs, discoveries, breakthroughs, surgery, laboratories, indemnity, inventions, copyright, trademark, local customs, asia, africa, europe, north america, central america, south america, down under, onshore, offshore, aerospace, aviation, contractors, subcontractors, developers, workers comp, schools, colleges, universities, student travel, travel assistance, hospitality, inventory, digital assets, security, failures, risk assessment, mergers, acquisitions, spin-offs, occupational accident, employer liability, entrepreneurs, employees, local, national, pilots, crews, business travel, foreign travel, vacations, emergencies, m trucking, healthcare, staffing, energy, environment, green, sustainability, renewable energy, carbon-capture ions, science, technology, imports, exports, inland, coastal, warehouses, real estate, mansions, cot engineers, consultants, land surveyors, pollution clean-up, pollution liability, premises pollutio storage tanks, boilers, machinery, auto parts, short term, long tail, loss control, catastrop limate risk, brownfields, disposal sites, water intrusion, defects, roofing, landscaping, pa roads, dams, crops, farms, errors, omissions, interruptions, utilities, cooperatives, captiv loss prevention, corporate assets, electronic media, broadcasters, publishers, media dis generating units, foreign suppliers, privately held, publicly held, non-profits, mid-size successor liability, discontinued products, spoilage, contamination, laser coverage, e xploration, production, distribution, electric, oil, gas, water, alternative energy, forgery management, supermarkets erships, trusts, subsidiaries, e armaceutical, clinical trials, er education, international t power, wind, hydro energy, railroads, light rails, food, beverage, radio, television, cars, drivers, fine art, jewelry, rare coins, antiques, medical, personal accident, group accident, supplemental health, banks, financial institutions, asset managers, investment banks, affinity groups, telemarketing, associations, clubs, societies, cruise lines, tour operators, sponsorships, partnerships, war risks, political risk, recovery, public, private, high-tech, e-business, progress, global, innovation, growth, flexibility, seamlessness, consistency, integration, accessibility, property, liability, public liability, excess casualty, directors, officers, leisure industry, airlines, travel agents, hotels, resorts, restaurants, bistros, cargo, containers, harbors, cranes, accident and health, life insurance, reinsurance, marine, charter vessels, commercial hull, mega yachts pleasure boats, whole life, term life, group life, disability, construction, skyscrapers, museums, public parks, offices, hospitals, agriculture, excess liability, medical malpractice, political risk, homeowners, automotive, fleet, 18-wheelers, vans, hybrids, motorcycles, scooters, school buses, estate, surety, products, damage, theft, landlords, lessees, retail, shopping malls, product liability, identity theft, data theft, data recovery, power stations, gas stations, refineries, drill islands, pipelines, natural gas, hydrogen, tankers, carbon waste, pollution, storage tanks, football clubs, cricket clubs, country clubs, discoveries, breakthroughs, surgery, laboratories, indemnity, inventions, copyright, trademark, local customs, asia, africa, europe, north america, central america, south america, down under, onshore, offshore, aerospace, aviation, contractors, subcontractors, developers, workers comp, schools, colleges, universities, student travel, hospitality, travel assistance, inventory, digital assets, security, failures, risk assessment, mergers, acquisitions, spin-offs, occupational accident, employer liability, entrepreneurs, employees,

worldwide, ACE insures progress

Property & Casualty | Accident & Health | Life

ACE takes on the responsibility of your risks so you can take on the responsibility of making things happen. We call this *insuring progress*. To find out how our people, financial strength, worldwide capabilities and flexible approach can work to insure your progress, visit acegroup.com/eu today.

insuring progress®

Introduction & Contents

WELCOME

THE NUMBER AND COST OF DATA BREACHES APPEAR TO BE RISING EACH YEAR. WHILE US incidents and costs are fairly well documented, it is more difficult to gain a full picture of the situation in Europe, since notification of potentially affected customers is not mandatory in all countries for all types of companies. This may change, however, as the European Commission seeks to tighten and harmonise data privacy regulations.

The Commission's proposals are the result of the technological developments and the growth in globalisation that have taken place since the current Data Protection Directive was introduced. Not least among these is the growth in cloud computing, which poses some particular risk management challenges.

Handing over-sensitive data to a third party inevitably carries risks. But these may be especially significant in view of the fact that the cloud is a relatively recent phenomenon. For example, it can be difficult to ascertain where data is stored in the virtual cloud environment, the robustness – or otherwise – of the cloud provider's security, and even in some cases whether the cloud provider is handling data in a lawful way. The traditional checks that companies run when outsourcing may be much harder to enforce.

The financial and reputational costs of a data breach can be enormous, and risk management plays a key role in minimising likelihood and potential losses. In addition to technological protections against system intrusions, more companies are finding the need to enforce controls to guard against internal risks.

Employees' actions – deliberate or unintentional – are one of the key causes of data breaches. For some risk managers, potential leaking of confidential information by employees on social networking sites is a particular concern. Companies are responding to the 'insider' risk by increasing awareness and in some cases establishing guidelines on social networking.

Should the worst happen, companies need to respond quickly and efficiently to minimise damage, which can include significant business interruption costs. Dealing with a data breach is becoming a crucial component when designing crisis management plans.

It is not surprising that today's increased focus on preserving data privacy has boosted interest in cyber risk insurance. In turn, some insurers have fine-tuned cover to meet companies' needs more precisely, for example covering the costs of forensic investigation into a suspected incident and offering panels of experts to help handle breach responses.

Patrick Pouillot, IT underwriting manager for continental Europe, ACE

Editor Nathan Skinner
Editor-in-chief Sue Copeman
Market analyst Andrew Leslie
Group production editor Áine Kelly
Deputy chief sub-editor Laura Sharp
Business development manager Donna Penfold
tel: +44 (0)20 7618 3426
Production designer Nikki Easton
Group production manager Tricia McBride
Senior production controller Gareth Kime

Head of events Debbie Kidman
Events logistics manager Katherine Ball
Publisher William Sanders
tel: +44 (0)20 7618 3452
Managing director Tim Whitehouse

To email anyone at Newsquest Specialist Media, please use the following: firstname.surname@newsquestspecialistmedia.com

SPONSORED BY

A new direction for data

As ever more of our personal information becomes globally available on online networks, the European Commission is working to tighten its data protection laws

KEY POINTS

01: Rapid technological changes mean that new legislation in the area is inevitable.

02: Major challenges to EU-wide legislation include lack of harmonisation and increased outsourcing.

03: The USA has already implemented proposed EU laws in the form of mandatory notifications for data breaches.

04: The public is largely aware of its rights to request, view and contest personal information.

05: Penalties for failing to observe data privacy laws can be severe.

THE EU DATA PROTECTION DIRECTIVE is currently under review. The European Commission believes that reforms are essential to bring the rules into line with the rapid technological changes that have been – and are – taking place. Increased data security is pivotal to the new legislation.

In November 2010, the Commission published its approach to personal data protection in the EU. This was centred on the fact that rapid technological developments and globalisation have profoundly changed the world and brought new challenges.

The Commission says that technology today allows individuals to share information about their behaviour and preferences easily and make it publicly and globally available on an unprecedented scale, citing the example of social networking sites "with hundreds of millions of members spread across the globe".

Cloud computing could also pose challenges to data protection, as it may involve the loss of individuals' control over their potentially sensitive information when they store data with programmes hosted on someone else's hardware.

At the same time, ways of collecting personal data have become increasingly elaborate and less easily detectable, the Commission has warned. For example, sophisticated tools allow economic operators to better target individuals thanks to the monitoring of their behaviour. And the growing use of geo-location devices and procedures allowing automatic data collection, such as electronic transport ticketing and road toll collecting, make it easier to determine the location of individuals.

Public authorities also use more and more personal data for purposes such as tracing individuals in the event of an outbreak of a communicable disease, preventing and fighting terrorism and crime, and so on.

Keeping up

While the Commission's research and consultation processes confirmed that the core principles of the current directive are still valid, they also identified new challenges for future legislation to address:

- The need to clarify and specify the application of data protection principles to new technologies, in order to ensure that individuals' personal data is effectively protected, whatever the technology used to process their data, and that data controllers are fully aware of the implications of new technologies on data protection.
- The lack of sufficient harmonisation between member states' legislation on data protection, in spite of a common EU legal framework. Stakeholders stress the need to increase legal certainty, lessen the administrative burden and ensure a level playing field for economic operators and other data controllers.
- The increased outsourcing of processing, very often outside the EU, which raises several problems in relation to the law that applies to the processing and the allocation of associated responsibility. Many organisations consider that current schemes for international data transfers are not entirely satisfactory and need to be reviewed and streamlined to make them simpler and less burdensome.
- Consensus among stakeholders that data protection authorities' roles need strengthening to ensure better enforcement of data protection rules.
- The need for an overarching instrument applying to data processing operations in all sectors and policies of the EU to ensure an integrated approach as well as seamless, consistent and effective protection.

A number of EU commentators have stressed the aspects of the proposed

INFORMATION COMMISSIONER REPORTS UK FAILINGS

MOST ORGANISATIONS IN THE PUBLIC and private sectors fail to understand the legal requirements for the storage of personal data, according to research from the UK Information Commissioner's Office (ICO) last year.

The ICO Annual Track 2010 found that just 48% of private and 60% of public sector organisations are aware of the need to store personal information securely. The research also found that just 14% of all organisations can identify the data protection principles unprompted, a fall of 8% on the same survey in 2007.

The survey did contain some good news. Around 90% of individuals have a clear understanding of their right to see information about them held by an organisation, up 15% since 2004. Some 84% know that they can request information from authorities through the Freedom of Information Act. Around 80% said that the Freedom of Information Act was "necessary", while 93% described the Data Protection Act in the same terms.

Information commissioner Christopher Graham explained that the importance individuals place on data protection should act as a warning to businesses. "Individuals are concerned about the collection and secure storage of their personal information. Ignoring data protection obligations is ignoring a key customer concern," he said.

'The cost of no action in the field of data protection is much higher than the cost of improving the rules'

Viviane Reding European commissioner

changes that they consider most important.

European commissioner for justice, fundamental rights and citizenship Viviane Reding is leading the process of reform. She has expressed concern that personal data can easily be stored and then even more easily multiplied on the web – but it is not easy to wipe it out. She said that people need to be confident that the information they commit to the internet can be removed in the future – the so-called 'right to be forgotten' – particularly as social networks continue to store ever-increasing amounts of personal information.

Reding has also admitted that changes in legislation are likely to mean higher costs of compliance for businesses. But she believes that companies have specific responsibility because data is often their main economic asset – and "the cost of no action in the field of data protection is much higher than the cost of improving the rules".

Looking to the USA

The European data protection supervisor Peter Hustinx has called for the introduction of mandatory data breach notifications – a move that seems highly likely in the current data regulatory climate. US law firm Marshall Dennehey Warner Coleman & Goggin states that a recent speech by EU deputy commissioner and director of data protection David Smith indicates that mandatory data notification requirements are inevitable. The EU has already moved some way on this with a new EU directive, amending the previous E-Privacy Directive, coming into effect in May 2011.

EU Directive 2009/136/EC requires providers of publicly available electronic communications services to notify relevant national authorities and, in some instances, affected individuals, of a personal data breach. Marshall Dennehey Warner Coleman & Goggin states that this directive's notification provisions are very similar to many of the existing state notification laws in the USA. For example, the directive:

- conditions individual notification requirements on a risk-of-harm standard;
- requires notification "without undue delay"; and
- defines "breach" in similar language to that commonly used in US notification laws.

The firm warns: "Considering these similarities, telecom companies operating in Europe will no doubt be looking to the notification compliance efforts of US companies that have successfully handled past breaches. While Directive 2009/136/EC does not explicitly provide for specific enforcement penalties comparable to the enforcement provisions of US notification laws, many EU member states have instituted fines and penalties for violations of laws enacted under the existing E-Privacy Directive. We expect to see similar fine and penalty provisions in the forthcoming breach notification laws enacted under Directive 2009/136/EC."

The penalties for failing to observe data privacy laws can be severe. Law firm Norton Rose says: "While the sanctions that organisations may face if they fail to comply vary from country to country, in developed economies sanctions range from criminal prosecution to fines levied by regulators. Regardless of the enforcement regime, for many organisations the damage caused by bad publicity resulting from a breach may dwarf any fine."

UK information commissioner Christopher Graham agrees. "Businesses need to show that they are taking data protection seriously. Failing to do so could not only lead to enforcement action, but to significant damage to their reputation." **SR**

CURRENT EU RULES

THE EU DATA PROTECTION DIRECTIVE (ALSO KNOWN AS Directive 95/46/EC) is designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. Key principles include:

- people whose data is being collected should be given notice of this,
- data collected should be used only for stated purpose(s) and for no others,
- organisations collecting personal data should not disclose or share this with third parties without consent from the subject(s) of the data,
- organisations must keep the personal data they collect safe and secure from potential abuse, theft, or loss,
- people whose personal data is being collected should be informed as to who is collecting that data,
- people should be given access to their personal data and allowed to correct any inaccuracies,
- people should be able to hold personal data collectors accountable for adhering to all of these principles.

EUROPE TAKES UK TO TASK

THE EUROPEAN COMMISSION IS bringing an action in the EU Court of Justice against the UK government over its alleged failure to fully implement rules relating to the confidentiality of electronic communications. The Commission says that existing UK laws do not comply because:

- the country does not have an independent national authority to supervise interception of some communications,
- UK law allows interception where the perpetrator has "reasonable grounds for believing" that consent has been given for this,
- probation of unlawful interception of data is limited to "intentional" interception only whereas EU law requires that all member states prohibit and introduce sanctions against all unlawful interceptions, regardless of intent.

CLOUD STRATEGY NEEDED

EUROPEAN COMMISSION VICE-PRESIDENT RESPONSIBLE FOR the digital agenda Neelie Kroes believes that it is down to regulators and member states to make sure that citizens can trust in the security of cloud services. "The protection of personal data is a fundamental right in the EU, and this demands several actions."

Kroes advocates cloud assurances that apply to all member states, and recommends new laws and codes of practice. Her remarks stem from the many grey areas associated with data security in the context of the cloud (see page 6). She explains that the Commission is working on a cloud computing strategy which needs the input of all EU authorities.

Past breaches, future trends

What types of companies are the most vulnerable to large expensive data security breaches? Incidents over the last 10 years or so may provide a guide

KEY POINTS

01: Data breaches are increasing in frequency and are costing businesses more every year.

02: Despite the costly risk to 'first timers', companies are more vigilant about system failures than data breaches.

03: The true picture remains unknown as notifications are not mandatory globally.

EARLIER THIS YEAR, JAPANESE company Sony suffered a massive data breach when hackers accessed personal information on 77 million PlayStation Network and Qriocity accounts. The company was forced to shut down its network for almost a month and has introduced a range of new security measures including an early warning system to alert it to any future attempt to penetrate the network.

This was one of the biggest data breaches to date and illustrates the vulnerability of companies conducting business online. However, generally outside of the USA and a few other countries where notification of consumers after a data breach is mandatory, information on breaches tends to be sketchy.

Since compulsory notification was introduced in the USA, there have been a vast number of incidents recorded. Many of these involve government and military facilities as well as healthcare providers and educational institutions. Not surprisingly, banks and credit card companies have also been targets. But any company that holds personal details on its customers may become a victim.

- In 2007, retail giant TJX revealed that hackers had stolen customers' credit and debit card information. Over 40 million records were affected and the attack is estimated by some security experts to have cost the company billions rather than millions of dollars.

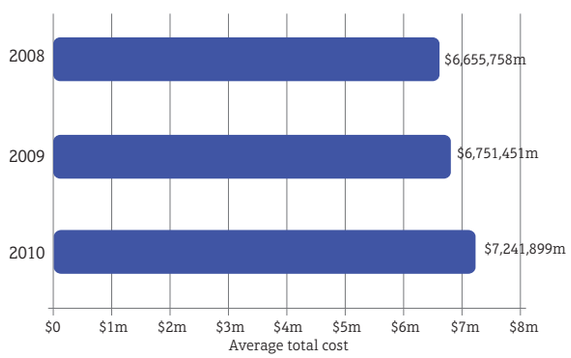
- In 2009, Heartland Payment Systems announced that hackers had stolen information on the 100 million or so transactions that it processed each month for merchants – once again at a huge cost to the business.

- Demonstrating that even smaller organisations' systems are not safe from intrusion, the US grocery store Hannaford Brothers reported in 2008 that hackers had gained access to more than 4.2 million credit card transactions. According to *InformationWeek*, by the time the breach was revealed more than 1,800 of the credit card numbers had been used.

- While many major incidents involve organised crime, dishonest employees can also cause significant damage. In 2007, Certegy Check Services, a subsidiary of Fidelity National Information Service, estimated that an employee's theft of customer records and subsequent sale to a data broker affected 8.5 million customers.

AVERAGE ORGANISATIONAL COST OF A DATA BREACH, 2008-10

Source: Symantec and Ponemon Institute



Counting the costs

Most data breaches affect thousands rather than millions of records. *The Ponemon Institute 2010 Annual Study: Cost of a Data Breach*, sponsored by Symantec Corporation, examines the costs incurred by 51 US organisations after experiencing data breaches ranging from nearly 4,200 records to 105,000 records from 15 different industry sectors.

Particularly interesting is the study's finding that, while more organisations favour rapid response to data breaches, a quick response generally adds to their costs. "In 2010, quick responders had a per-record cost of $268, up $49 (22%) from $219 the year before. Companies that took longer paid $174 per record, down $22 (11%) from 2009," says the report.

The institute believes that this suggests that moving too quickly through the data breach process may cause cost inefficiencies for an organisation, especially during the detection, escalation and notification phases.

Another key finding is that, in 2010 for the first time, malicious or criminal attacks were the most expensive cause of data breaches and not the least common one. "The 2010 cost per compromised record of a data breach involving a malicious or criminal act averaged $318, up $103 (48%) from 2009 and the highest of any data breach cause this year. The huge increases reinforce the extreme danger hostile breaches pose."

But US organisations are more proactively protecting themselves from malicious attacks. And breaches due to systems failures, lost or stolen devices and

third-party mistakes have reduced. Companies appear to be becoming more conscientious about preventing data breaches in the worsening threat environment.

The report also says that companies' investments in finding and remediating data breaches may be paying off by minimising the cost of lost business.

On the horizon?

Data security company Imperva has compiled 10 top security predictions for 2011 to help businesses protect themselves against the next onslaught of cyber security threats.

1. Nation-sponsored hacking and specifically targeted cyber attacks will incorporate concepts and techniques from the commercial hacker industry. But they will not be aimed at gaining financial advantage. For example, Stuxnet was focused on gaining control of crucial infrastructure. Companies with good security controls may be protected partially from advanced persistent threat (APT) attacks.

   But Imperva warns that, as APT is persistent, if a certain attack does not succeed, another one will come into play. "The traditional security controls do not deter these relentless, state-sponsored hacker organisations. For the enterprise as well as government, this means increasing monitoring of traffic and setting security controls across all organisation layers," it says.

2. There will be growing awareness to security incidents of an 'insider job' nature as a result of an increased flow of incident reports where data theft and security breaches are tied to employees and other insiders.

3. The sophistication of Man in the Browser (MitB) attacks will increase. While avoiding infection by proxy trojans is presumably the responsibility of consumers, MitB attacks are quickly becoming a concern of online service providers that need to be able to serve (and protect) customers who might be infected with malware.

4. Prominent social networks, and tools, will direct more efforts into security over privacy, reflecting an understanding of the real threats to the existence and proliferation of social networks. Security measures will provide improved protection against application layer attacks, stronger authentication and account control features, as well as better malware detection systems.

5. There will be a growing number of data breaches where compromised information is in the form of files rather than database records. Imperva says that, since each file is an autonomous entity, with respect to content ownership and access control (contrary to a database record), maintaining control of who can access a file is almost impossible, as is keeping track of access to those files that contain sensitive information. "The inability to maintain control may result in excessive access privileges and an inadequate audit trail of access to sensitive information."

6. There will be more application security offerings in the cloud throughout 2011, and Imperva predicts some early data security in the cloud offerings. Challenges include maintaining bulletproof partitions between datasets of different customers and providing different levels of data security to applications sharing the same logical or physical platforms.

7. The proliferation of sophisticated mobile devices will have a substantial effect on application and data security, in particular as organisations struggle to accommodate the increase in number and variety of these devices, while maintaining traditional data and application security practices. Imperva expects "exponential growth" in the number of incidents related to mobile devices in the next few years.

8. Security researchers will continue to look into the hacker operations and will unearth the smaller or less diligent criminals. In general, the hacker industry will react by investing more resources in attack techniques and detection evasion. The hackers that cannot make this investment will go out of business. Other cyber-criminal organisations will 'buy out' other groups or merge their operations with others.

9. Cyber security will become a business process. "This means security teams need to become business process experts to keep the bad guys disarmed while keeping the good guys productive," says Imperva.

10. There will be convergence of data security and privacy regulation worldwide. With companies finding the task of complying with multiple mandates across borders very difficult, governments are already beginning to define a common framework to make life easier for themselves and for enterprises housing data. **SR**

OVERALL TRENDS

The Ponemon Institute 2010 Annual Study: Cost of a Data Breach identified the following trends:

- Breach costs directly reflect IT security best practices and threat trends. Data breach costs more or less correlate directly with the presence or absence of major data breach causes (malicious attacks, for example) or data protection best practices (such as chief information security officer (CISO) leadership).
- Data breaches continue to cost organisations more every year.
- Customer turnover in direct response to breaches remains the main driver of data breach costs.
- Training and awareness programmes remain the most popular post-breach remedies, but encryption and other technologies are gaining fast.
- Breaches by third-party outsourcers are becoming slightly less common but much more expensive.
- Breaches involving lost or stolen laptop computers or other mobile data-bearing devices remain a consistent and expensive threat.
- Companies are more vigilant about preventing systems failures.
- Negligence remains the most common threat, and an increasingly expensive one.
- 'First timers' pay the highest breach costs because they often lack breach response experience that can help lower costs.
- To better manage data breaches and reduce breach costs, more companies are trusting their CISOs.
- Fewer organisations are using external consulting support, even though such support lowers data breach costs. Organisations in a rush to respond may not believe they have the time to bring in outside help to meet compliance requirements. This in turn could help explain the increase in popularity of relying on CISOs, as organisations can quickly leverage these internal resources and see similar cost benefits.
- More companies had better-than-average security postures, and those organisations enjoyed much lower data breach costs.

Taking control of the cloud

With significant cost benefits, storing data in 'the cloud' is an attractive idea, but as a relatively new concept and with no universal governance, it is not without its risks

KEY POINTS

01: Storing data in the cloud poses a variety of risks that many risk managers have not considered.

02: Experts suggest transferring risk to cloud providers, but this cannot cover reputational damage or legal implications.

03: A lack of universally accepted standards and protocol creates a further challenge.

04: Moves are afoot to implement an industry-standard cloud certification programme.

05: Always check a cloud provider's controls and standing.

CLOUD COMPUTING CAN OFFER significant cost benefits – but these may come at a price. Director of information security practice at PricewaterhouseCoopers UK William Beer warns that cloud computing in its broadest terms presents new areas of risk that a lot of organisations have not completely come to grips with yet. "The main cloud providers have been focusing on things like scalability, technology, flexibility and of course cost savings. There hasn't really been much active discussion on information security."

ACE European Group (UK) cyber underwriter Iain Ainslie summarises the problem. "If your data is stored within your own building, with your own staff looking after your servers, you have an element of control. If that information is in the cloud, you are relinquishing your control."

Out of your hands

Two years ago, when the EU's European Network and Information Security Agency (ENISA) looked at the benefits and risks associated with cloud computing as part of its emerging and future risk programme, it identified the following major security risks:

- **Loss of governance.** In using cloud infrastructures, the client necessarily cedes control to the cloud provider on a number of issues that may affect security. At the same time, service level agreements may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences.
- **Lock in.** The lack of tools, procedures or standard data formats or services interfaces that guarantee data, application and service portability may make it difficult for customers to migrate from one provider to another or bring data and services back in-house.
- **Isolation failure.** Mechanisms separating storage, memory and routing between different tenants could fail.
- **Compliance risks.** Investment in achieving certification (for example, industry standard or regulatory requirements) may be put at risk by migration to the cloud if the provider cannot evidence its own compliance with the relevant requirements or does not allow the customer to audit.
- **Management interface compromise.** Customer management interfaces of a public cloud provider are accessible through the internet and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.
- **Data protection.** In some cases, it may be difficult for the cloud customer in its role as data controller to effectively check the data-handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way.
- **Insecure or incomplete data deletion.** When a request to delete a cloud resource is made, this may not result in true wiping of the data. Adequate or timely deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients.
- **Malicious insider.** While usually less likely, the damage that may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles that are extremely high-risk, for example system administrators.

ENISA says that it is often possible, and in some cases advisable, for the customer to transfer risk to the cloud provider. But a customer cannot transfer all risks, for example serious damage to reputation or legal implications. "Ultimately, you can outsource responsibility but you can't outsource accountability," warns the agency.

While Beer concedes that a lot of the traditional approaches in terms of doing due diligence can apply, he cautions that it can

MOVES TOWARDS CERTIFICATION?

THE CLOUD SECURITY ALLIANCE (CSA) OPENED ITS CERTIFICATE OF CLOUD SECURITY Knowledge (CCSK) for testing last year. Described as the industry's first user certification programme for secure cloud computing, the CCSK is designed to ensure that a broad range of professionals with responsibility related to cloud computing have a demonstrated awareness of the security threats and best practices for securing the cloud.

CSA says that, as cloud computing is being aggressively adopted, it is critical that the industry provide training and certification of professionals to ensure that cloud computing is implemented responsibly with the appropriate security controls. The programme reflects both CSA's own catalogue of security best practices, the Security Guidance for Critical Areas of Focus in Cloud Computing, and ENISA's recommendations.

be easy for an individual within an organisation to bypass due diligence by going to a public cloud provider and using their corporate credit card to buy services on their own. "That would bypass all the things that your organisation has in place and it makes some of the traditional approaches very difficult to apply," he says.

Data difficulties

Beer sees one of the key risks that organisations face relate primarily to data privacy. "Where is data stored and located?" he asks. "Most cloud providers are struggling to provide assurance and concrete evidence as to where data may come and flow due to the technical nature of the cloud, which uses virtualisation technology. This makes it extremely hard for them to say whether data is being stored in the USA, UK or wherever. It is a massive challenge that most of them are still struggling with."

Ainslie points out that certain provisions apply where European companies' data is stored outside of the EU. "It's important to make sure that storage arrangements are acceptable," he says.

Another major problem that Beer identifies is the lack of the universally accepted service standards and certification that normally apply when using a third-party provider of computer services. "These can provide an organisation buying traditional data services with some comfort, as well as reassuring any regulatory authorities involved. But the cloud environment based in virtualisation technologies means that these standards may not necessarily apply. There's currently a great deal of debate as to whether a specific new cloud standard is needed."

He also picks up on two of the issues identified by ENISA: lock-in and insecure or incomplete data deletion. Beer says: "Cloud computing provision is a relatively new space. There are quite a few providers. Some will probably go bankrupt; some will be acquired. Because there are no standards on intercompatibility or sharing information what happens then? This new sector does not have many answers here yet. And if information needs to be deleted, what assurance can they provide that your data has been safely destroyed?"

There is also a question mark around the availability of 24/7 support. "What sort of guarantees can cloud providers give that important services are going to be available?" Beer asks. "A lot of the providers, particularly the newer ones, have structured their service level agreements in a very modular way and are inflexible when it comes to modifying their contracts."

Ensuring model alignment

Ainslie urges companies to drill down into the cloud provider's business approach. "You may be using a SaaS provider, putting your data into a software tool in the cloud to take advantage of benefits such as cost and scalability. But you need to be aware that your provider may have the same business model and be using another company's services – which means that your data may be sitting with the vendor of your vendor.

"You need to ask if your vendor is using another party, who they are and whether it is possible to audit them to check their controls and standing. And with both direct and indirect vendors, you need to be able to check that they have insurance to compensate you for any data breach that you suffer as a result of their negligence."

He also warns that, while you may seek to protect your data held in the cloud by encryption, it is not uncommon for your cloud provider to ask for the keys to the encryption. "Once you give the keys away, is that data still secure?" Ainslie asks. "If your cloud provider asks for keys, ask them why they need them and how they intend to store them."

Additional risks

In its June report, *Assessing the Security Risks of Cloud Computing*, Gartner says that sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT retailers exert over in-house programmes. The firm recommends users to get as much information as they can about the people who manage their data.

Gartner also warns that investigating inappropriate or illegal activity may be impossible in cloud computing. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centres," says the report.

Ainslie concludes: "It's essential to ensure that the service given by your cloud provider is more than just a cost-cutting exercise but a secure and reliable service as well." **SR**

DEFINING CLOUD COMPUTING

There are three categories of cloud computing:

- Software as a service (SaaS): is software offered by a third-party provider, available on demand, usually via the internet configurable remotely. Examples include online word processing and spreadsheet tools, CRM services and web content delivery services (Salesforce CRM, Google Docs, and so on).
- Platform as a service (PaaS): allows customers to develop new applications using APIs deployed and is configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms. Examples are Microsoft Azure, Force and Google App engine.
- Infrastructure as service (IaaS): provides virtual machines and other abstracted hardware and operating systems that may be controlled through a service API. Examples include Amazon EC2 and S3, Windows Live Skydrive and Rackspace Cloud.

Clouds may also be divided into:

- Public: available publicly – any organisation may subscribe.
- Private: services built according to cloud computing principles, but accessible only within a private network.
- Partner: cloud services offered by a provider to a limited and well-defined number of parties.

Source: Cloud computing – benefits, risks and recommendations for information security, *November 2009, ENISA*

CLOUD CRASH

AMAZON WEB SERVICES' SIGNIFICANT PERIOD OF OUTAGE IN APRIL ILLUSTRATES THE risks for users that depend on cloud technology. The incident took down many other online sites and internet services that rely on Amazon's cloud.

The outage was caused by a glitch at the company's northern Virginia data centre. Some block storage volumes created new backups of themselves, which filled up Amazon's available storage capacity, leading to connectivity problems.

Users affected included: question and answer site Quora, social media hub Reddit, the HootSuite link-sharing tool, and location-based services Foursquare and SCVNGR.

Prevention and cure

No company is able to boast completely bullet-proof data security provisions, but it is possible to mitigate breach risks efficiently

KEY POINTS

01: Causes and consequences of data breaches should be graded for probability, indicating where risk is greatest.

02: Data breach scenarios should be written into crisis management plans.

03: Should a breach occur, evaluate the situation thoroughly before reacting, lest further damage – both reputational and legal – occur.

COMPANIES' IT EXPERTS AND advisers may be smart but the high incidence of data security breaches suggests that hackers may be smarter, while dishonest or careless employees also remain a threat. So just how should companies approach data risk management and minimise the downside should a breach occur?

Head of Marsh Risk Consulting in France Marc Paasch suggests that an important first step is to identify and analyse the possible scenarios that could result in a breach or loss of data. "These could include a range of incidents such as hacking, loss through fire or a natural catastrophe, and even malicious damage," he says.

In connection with the latter, Paasch gives the example of a head of IT who takes your systems' codes when he leaves the company and then uses these codes to change some information in your databases. "It's usually possible to detect any erased information fairly quickly but relatively small alterations can be quite difficult to spot," Paasch says.

Having identified the possible causes and consequences in terms of both financial and reputational loss, these should be graded for probability. This will highlight the potentially very damaging losses that have a reasonably high chance of occurring and will give an indication of where the risk is greatest, explains Paasch.

"For example, we recently completed a study for a very large European company. This was not in one of the traditional high-risk sectors like financial, telecoms or retail, but nonetheless it held data on over one million clients," says Paasch.

He continues: "We identified two major risk scenarios. The first was that client data might be stolen. The second was that hacking of their overall systems would allow criminals to transfer payments to bogus accounts. Providing this kind of risk information allows a company to set up the right kind of controls to prevent occurrences – and plan the right level of crisis management should the worst happen."

Layers of security

Paasch advocates a multi-tier approach to risk management. The first involves the human element, asking the right questions to assess whether you need to improve controls. He says: "Look at who is entering and exiting the systems. When are the codes changed? Which individuals have access to what? Who handles your systems maintenance?"

On the human angle, ACE European Group (UK) cyber underwriter Iain Ainslie says that it's important to make staff aware of what constitutes sensitive material and the degrees of sensitivity that may apply. He suggests: "You can do this with a range of measures including training videos with tests at the end to ensure the message has gotten across, and awareness campaigns. But you need to run regular checks to make sure procedures are policed."

Employees need to understand the potential implications of data breaches. "Risks to their company could ultimately affect their own jobs and if they understand this, they may take more care," he says.

Secondly, you should consider physical and virtual protections. How easy is it for unauthorised people to gain access to your premises where data is stored? What back-up facilities, anti-virus protections and firewalls does your company's IT systems have?

Ainslie warns that it's important not to be too reliant on technology – even if it is the latest model. "When a new firewall comes on the market, hackers will buy it, work out a script to breach it and then send that over the net to find and attack firewalls of that type. For this reason, it's important to have layers of security – if one is breached, there's another underlying it," he says.

Ainslie suggests another strategy of not putting all your data on one server. "Try to distribute it around several servers so if one is breached you don't lose everything."

Basic measures

Patrick Donnelly, managing director of professional risk solutions for Aon Risk Solutions' Financial Services Group, also advocates a structured approach to managing data security risks. He stresses the advantage of using the same basis as that applied to other corporate risks so that it is familiar to both the company and its risk management team. He explains that this includes:

- risk identification,
- risk assessment,
- evaluating the efficacy of risk controls,
- quantifying the exposure that remains after assessing efficacy, the appropriateness of risk transfer or other risk financing, and
- designing a framework to manage the residual risk that remains after any risk transfer.

"While you take these same basic steps, it is of course important to apply specifics in the context of managing data privacy," he says. "For example, companies will need to

'Establish a relationship with an appropriate crisis management public relations firm so that you can call upon them if there's a problem'

Iain Ainslie ACE UK

establish their standards for risk assessment. These may be by industry or size of company but there may also be some general standards that apply within the particular industry sector."

Donnelly cites the retail sector which, in connection with credit card payments, needs to comply with the payment card industry's data security standards. The International Organisation for Standardisation has also developed a code of practice for information security management. "ISO has around 162 member countries so this is a standard that is fairly well recognised by companies and information security professionals globally," says Donnelly.

Another step in the risk assessment process is to look at the company's latest third-party or internal audit. "The findings of your latest report on compliance will be fundamental here," he states.

While establishing the standards against which to assess your risk may be relatively straightforward, evaluating the efficacy of risk controls is not quite so defined, warns Donnelly. "Controls tend to focus in three areas," he explains. "It is important to look at the efficacy of risk controls in the context of contractual controls, operational controls and technological controls."

There has been quite a significant change here since companies first started to focus on data privacy risk management. "Initially, companies concentrated on the technological aspects with information risks being largely managed by their IT departments.

"Most organisations have moved on from that, understanding that technology is only part of the picture. So there is focus now on operational controls as well, taking in aspects such as who has access to data and increasing employees' risk awareness, for example by training. Companies have come a long way in understanding how risk controls can help manage the identified risks," says Donnelly.

Quantifying the risk

Risk exposure quantification can take several forms. Most companies look at third party issues, look at their own experience and also take into account publicly available information. This may well be the approach adopted by companies in sectors which are not deemed to have the highest exposure – perhaps because they store little or no personal and financial information on their customers.

But Donnelly says that some companies require a more specific, even actuarially driven, quantification of risk, modelling their portfolios of personal privacy risks. "Once the model is established, they can overlay various risk financing treatments to help the company come to the optimal view of how to finance the risk," he explains.

Alongside questions concerning the robustness of your IT protection has to come the consideration of how much your company wants or needs to invest in it. Paasch explains: "For an industrial client as opposed to, say, a financial institution or a telecoms company, losses arising from a data breach are probably not going to be that great and will represent a far smaller share of their total cost of risk.

"So the amount of money they invest in IT protection is likely to reflect this, along with their tolerance or appetite for this type of risk. They need to reach a solution that they feel comfortable with."

Ainslie agrees that companies need to analyse the costs versus the benefits. But he gives an analogy: "If you live in a row of 10 houses and everyone goes on holiday, the one that leaves the windows and doors open is more likely to get burgled!"

Basic precautions are important and, in any event, you need to make sure that whatever controls you put in place are reviewed regularly.

Once the risk management approach, controls and any risk transfer are in place, the company needs to establish how it would deal with a data security breach. There is general consensus among risk advisers – and some risk managers – that no system is fail-safe because the extent of the controls required to achieve this would be counter-productive to the efficient running of the business itself. "A planned, organised approach to dealing with any data breach is the final component in risk management planning," Donnelly says.

"Your business continuity and crisis management plans should take account of what you need to do should there be a data breach," Paasch says. "There are no hard and fast rules because circumstances and the types of information involved vary, but generally it is important to be as transparent as possible. Notifying any clients that could potentially be impacted can often save problems at a later stage," he explains.

Respond reasonably

Ainslie agrees but warns companies to not act too hastily. "A lot of businesses get into trouble because they do the wrong thing. For example, there have been cases where companies have panicked after they have discovered a data breach and notified all the customers that they think might be involved.

"Later investigation has shown that the breach was not as serious as they thought and they have then had to send out another notification, doubling their costs and potentially damaging their reputations," he says.

Ainslie also recommends that you line up in advance the people that you might need to rely on should a serious data breach occur. "Establish a relationship with an appropriate crisis management public relations firm so that you can call upon them if there's a problem," he says. "Contacting people and trying to enlist their help at the last moment when there is a real panic situation will almost always be more expensive and less effective." **SR**

TOP TIPS

1. Don't just rely on technology to protect your data – restrict access to sensitive information and train employees to be risk aware.
2. Identify and risk manage the potentially very damaging losses that have a reasonably high chance of occurring.
3. Align investment with potential loss – including any reputational damage implications – so that you don't over spend or skimp on essentials.
4. Assess your exposure and the standards you need to apply in the light of reported losses in your business sector and best practice guidance.
5. Run regular checks to make sure controls remain in place and employees are adhering to protective strategies.
6. Make dealing with a data breach part of your business continuity and crisis management plans.

Security service

Cyber risk insurance has become a must-have, as companies start to realise the full ramifications of a data breach and that no organisation is safe

KEY POINTS

01: Hacking is often indiscriminate, affecting smaller companies as well as larger ones.

02: Notifying all potentially affected companies when a data breach occurs – which is set to become mandatory under EU law – can be extremely expensive.

03: The rise of social media has increased the likelihood of confidential data being leaked inadvertently from within.

CYBER RISK INSURANCE HAS TAKEN some years to become established among European companies. But recent trends have pushed it up the risk management agenda.

The purchase of cyber risk insurance had a boost at the end of the 1990s because of fears that the millennium bug could hit businesses hard. When this didn't happen, it tended to take a back seat. But a number of recent changes have highlighted the importance of the cover and it is now being described in some quarters as the "new D&O" (that is, a cover once considered irrelevant in Europe and now seen as a must-have).

ACE European Group (UK) cyber risk underwriter Iain Ainslie explains: "In the last 10 or 11 years, companies have come to rely more heavily on IT than before. As a consequence, an IT problem can be a major issue, affecting their revenues and balance sheets."

But it is not just the growth in importance of IT that has alerted companies to the need to protect themselves. Ainslie points out that some European jurisdictions such as the UK are becoming far more litigious. Criminals too are becoming more aware of the value of data and, with so much held online, it is easier to get to if you do not protect it. "Hackers sell it on to other criminals, who know what to do with it and commit the actual fraud," Ainslie warns.

Mixed motives

In addition, a number of high-profile IT security breaches have focused corporate attention. Although it is the incidents affecting the largest companies that have hit the headlines, Ainslie warns that smaller companies should not consider themselves safe. "A hacker will send a script around the web that tries to find holes in the security of any company – and there are more of these attacks than the targeted hacking that we tend to read about."

But targeted attacks are still a serious issue for some companies – and ACE IT underwriting manager for Continental Europe Patrick Pouillot says that in some cases there is a change in motivation. "Attacks on data security now are not just coming from criminal or political organisations but also from aggrieved individuals who consider that a particular company has done something wrong and want to punish it," he says. "This could mean that we will see some new viruses that specifically target one company, which would be difficult for traditional risk prevention techniques to combat."

Pouillot cites Stuxnet, a worm that initially infects Windows machines and then goes on to seek out industrial control software made by Siemens. It then reprograms the software to give machinery new instructions. "It is evident and provable that Stuxnet is a directed sabotage attack involving heavy insider knowledge," says industrial computer expert Ralph Langner in analysis published on the web.

While the focus tends to be on online attacks by hackers, it is a mistake to think that data security attacks are always so sophisticated. As long as their methods work, criminals tend not to be too worried about how they get hold of the information. For example, they may get branded memory sticks reproduced, leaving these in company car parks or outside offices. Ainslie says: "Employees pick them up, thinking they've been dropped by a colleague, and then plug them into their PC to try to see who they belong to, unwittingly unleashing a virus into the system."

A duty to report

There is likely to be even more increased attention on security and protection when

EXPOSURE TO THIRD-PARTY CLAIMS

THIRD-PARTY CLAIMS ARE NOT ALWAYS THE DIRECT RESULT OF DATA BREACHES.

- Most employees use their work PCs to make purchases, visit websites, check their personal emails, and so on. They could pick up a virus in the course of their browsing, which would affect your company's systems and the emails sent out.
- If people in your company send out emails with viruses attached and the result is that recipient individuals or companies experience a financial loss, they can claim against you for this.
- IT forensic experts can determine the origin of such viruses.
- Currently ACE provides cyber insurance covering first-party loss and third-party liability in the UK and across continental Europe, even if the insurer's policies offered in Europe can vary from one insurance market to another in terms of cyber, media and privacy liabilities.

proposed EU legislation comes to fruition. In an effort to harmonise approaches across member states, the European Commission looks set to make it mandatory to notify potentially affected customers of all companies when a data breach occurs – not just those in the recognised high-risk categories.

Notifications can be very expensive if large numbers are involved and companies often also have to pay legal advisers to make sure that they couch their message in the right way.

'Attacks on data security now are not just coming from criminal or political organisations but also from aggrieved individuals'

Patrick Pouillot ACE UK

But, even at present, Pouillot says that most insurers will respect the views of their clients' risk managers as to whether to notify or not after a significant data breach. "The notification costs may be huge but quick notification could prevent liability claims. It's a question of trying to prevent the impact of the incident on the customers in both the company's and the insurer's interests," he says.

What's 'sensitive'?

Serious data breaches involve "sensitive" information – but how do you decide just what falls into this category? Clearly personal customer information such as credit card and bank details needs to be protected. Less obvious but still sensitive are customers' names and email addresses. Obtaining these could allow criminals to send scam information and phishing emails.

But it's important to remember that some of your own company's data is sensitive, too. Although the legislative focus has been on protecting individuals and clients, reflected in the third-party cover offered by insurers, your company itself could suffer significant loss through a data breach involving its own business plans and strategies.

No company would want to share its innermost trade secrets and business plans with its competitors. But a successful data breach could mean that you end up doing just that.

Accidental leaks

There are many ways that your company's confidential information could be "leaked". But one that risk managers are increasingly aware of is through social networking sites.

Organisations use social media sites quite extensively and often encourage their employees to do the same and blog on their own or other sites as appropriate. It's a way of getting their business and services known, with a potentially huge audience and at a far cheaper cost than traditional advertising.

But they could be swimming in shark-infested waters, because there is no certainty about protection should anything go wrong. "There is not much case law and no set rules about issues like intellectual property protection, defamation and leakage of confidential information yet," Ainslie says. Certainly it makes it a difficult area for insurers to provide cover.

Companies do have some control over their own pages on Facebook and similar sites, in that they can remove inappropriate content quickly and easily. If your employee posts a message, inadvertently giving away confidential information about your company, your options are not so clear.

You might be able to take action against that employee on the grounds that they have breached their confidentiality agreement with your business. But if a rival company uses this information to your own company's detriment, there may be little you can do, as their argument will be that the information was in the public domain.

Pouillot says that one of the challenges that insurers face lies in the new types of claims that may be presented. "We all tend to think in absolute terms – that a breach or other problem has been discovered that needs correcting – but sometimes it's not that simple. The IT manager may go into the office on Monday morning and consider that something in the systems does not feel right but he's not quite sure what may have happened over the weekend."

Pouillot believes that in the future there will be a greater demand for insurers to cover the costs of investigating whether a loss has actually occurred. He says: "It will change the definition of claim in this area of business." **SR**

A CONSULTANT'S VIEW

PATRICK DONNELLY, MANAGING director of professional risk solutions for Aon Risk Solutions' Financial Services Group, comments: "There has been an evolution in the insurance cover available in the last two years or so. When the initial cyber policies were introduced in the late 1990s, they were fairly restrictive, focusing on network security liability coverage and first-party property insurance, which very much resembled traditional property insurance cover although linked to non-physical perils.

"Over the years, this has changed to the extent that insurance cover now adds much more value. The first-party cover – the insurance for losses of the organisation – is no longer limited to replacing assets or providing business interruption cover, but can include reimbursement for the costs associated with investigating a breach event and managing the breach response.

"As a result, we've seen a trend in the last six months with organisations willing to take higher retentions on the front end of the cover but looking to build fuller coverage rather than sub-limits within the elements associated with breach response events. And some insurers are not only willing to offer reimbursement for breach response costs but also offer access to a panel of experts with experience in managing breach incidents.

"Liability coverage has moved beyond responding to damages arising from specified network perils to include a broad trigger for damages arising from the breach of any duty to keep information from improper or inadvertant disclosure. While policies have always responded to defence costs and damages associated with third-party claims, coverage may now be tailored to also respond to costs and damages arising out of a regulatory investigation or enforcement action.

"At a time of unprecedented capacity, the cost of cyber risk insurance is more attractive than it has ever been. That is proving to be incredibly compelling for companies of all sizes in all industries. No organisation can be 100% sure that it won't have a problem."

First line of defence

Data privacy should be a top priority for risk managers, but no company can boast a 100% security assurance. They can, however, learn valuable data protection lessons from others

KEY POINTS

01: Having a data back-up is vital, but be sure not to store it near the main system, and ensure it has wide compatibility.

02: Any system that is developed by people can be cracked by people; therefore grant access permissions cautiously.

03: By embracing social networking with guidelines and training, accidental data slips can be avoided.

PROTECTING DATA PRIVACY IS AN important issue for virtually all companies. Even those that do not store individuals' personal data within their IT systems are concerned to protect confidential information regarding clients and contracts that could be valuable to a competitor. And ensuring reliable and robust technology is essential for many other corporate functions as well.

Katoen Natie chief risk officer Carl Leeman says: "There is probably not one business today where IT has not increased in importance. Certainly in the logistics business that I am involved in, we have warehouse management systems that are very important. Any problem with our IT system there would quickly result in major problems."

Leeman considers there to be a number of IT risks, particularly in relation to information security, even for companies that are not apparently in the highest risk areas. He warns that relying on your back-up system may be dangerous. "Most companies have a back-up system but not all of them can be sure that they will work, for several reasons," he says. For example, it is a common mistake to store the back-up in the same building as the main computer system, as a disaster such as a fire may destroy both.

Leeman also believes that having a back-up that is specific to your particular system can be a mistake. "Some companies have a back-up that works only on their mainframe. If the mainframe is damaged the back-up will be useless because the system to drive it is dead," he warns.

In addition, he says that reports suggest that many back-ups – perhaps around 20% – just don't work properly for a variety of technical reasons.

Other IT risks he cites include intrusion, for example by viruses, and inappropriate use of the company's network by employees. "Every system that is developed by people can be cracked by people. We have seen that all types of very heavily protected IT systems have been hacked into – even the US White House computer system."

He also refers to the reputational damage that can occur if companies don't 'clean up' old websites. "Sometimes companies register a number of different websites in various names. They abandon some of these and other businesses or individuals take over the name and use the websites for unacceptable purposes," he says.

Leeman says his company's system does not hold personal data like individuals' addresses. "But we do hold technical information on contracts. I have been assured it is impossible for this to be downloaded by people with bad intentions or employees who leave the company.

"There are a number of controls in place. These include limiting the number of people who can view this information and restricting even further those with the ability to download it. For example, people working in one business unit cannot view contracts issued by another business unit."

Like Leeman, Prysmian Group group risk manager Alessandro De Felice works for an industrial company not a high-risk sector, so his data security concerns also focus around corporate confidentiality rather than leakage of individual consumers' private information. "Risk perception varies a lot according to business sector," he says.

De Felice explains that his company relies on its IT system to provide accurate and prompt financial and other data. "Protecting our data, for example in terms of customers' invoices, is a major consideration that is directly related to our business continuity," he says. "It is fundamental to establish a procedure and a framework where IT risks are properly managed, so our investment in IT is significant. Our data protection is facilitated through cross-department activity. Our IT, security and risk management departments are all involved – there's no single owner of the risk."

Strategies include control procedures for employees to prevent loss of data, controls to prevent external intrusion and also general physical protections to prevent unauthorised access and damage to the systems.

Personnel security

Elaine Heyworth is the former head of risk management of Everything Everywhere, a UK telecoms company formed by the merger of Orange and T-Mobile. The latter suffered a data security breach two years ago, when two employees stole customer data and sold it on to rival firms. "The company had to work very closely with the Information Commissioner's office to manage that breach. For us it became much more critical to look at our internal employees, and it was the start of a whole range of changes around personnel security," Heyworth says.

Extra layers of protection were added to ensure that no single employee had access to the data, with two or three employees having to sign off before someone could access information. "The information security team also introduced security for laptops and computers that meant that no employee could use a non-encrypted portable memory device and memory sticks were only designed to operate for transferring data from one employee's PC to another employee's PC," Heyworth explains.

ONLINE IN PRACTICE

For more practical advice on dealing with risk management challenges within your organisation, visit www.strategic-risk.eu/in-practice

'The fact that the two employees involved in our breach were prosecuted and went to prison signalled how seriously we take data security'

Elaine Heyworth formerly Everything Everywhere

There was a general campaign supported by the management team and board to create more data security awareness accompanied with training across the business. "We needed to make people aware of the implications of security failures or deliberate breaches. The fact that the two employees involved in our breach were prosecuted and went to prison signalled how seriously we take data security."

The company is a member of CIPSIE (the Communications Industry Personnel Security Information Exchange), run by CPNI (the government's Centre for the Protection of National Infrastructure). Since its data breach, it has looked far more deeply into the trustworthiness of its employees, exchanging information with other mobile phone companies.

Inevitably, the breach led to a tightening of external controls as well, with added layers of security around the company's networks and customer database.

Heyworth concludes: "For any retailer, its customer information is a critical part of its infrastructure. But the fact is that – unless you are very lucky – you cannot completely guarantee that your business is secure from the actions of a rogue employee. You just have to try to put in as many controls as you can without restricting business flow."

In the meantime, Russian telecoms companies are struggling to meet the requirements of a strict new law that imposes onerous guidelines as to what these companies have to do to protect their subscribers' data and personal information.

Mobile Telesystems OJSC head of risk management Igor Mikhaylov says: "Like most companies in this sector, we have certain security measures protecting our system and we train those of our people who have access to the sensitive data. We have a special department headed by our vice-president of security that is responsible for this. But the new law is tough and hard to comply with. The level of security is comparable to that relating to top-level government secrets, which may be over-excessive.

"My company operates in around 80 regions in Russia as well as in several other countries. All our systems in all the regions where we operate have to be secured to the standards laid down by the new law. But we do expect some changes to be made because of the difficulties associated with compliance."

The penalties of non-compliance would be very substantial, says Mikhaylov. "Users might not be prevented from using our services but our reputation could certainly be affected on a local basis in the regions where we operate."

Social networking risks

It is not just the risks of hackers gaining access to information or rogue employees that are taxing the minds of European risk managers. The danger of information being inadvertently leaked by employees through social networking was addressed at October's Ferma Forum in a session called 'The risks of the virtual world'.

Moderator Michel Dennery, deputy chief risk officer at GDF Suez, opened the discussion by saying that information is an open door in computerisation. "Who accesses the information, what is the value of the information and could your competitors gain competitive advantage if they had it?"

Bureau Européen d'Information Commerciale secretary-general Laurent Delhalle warned that companies have to consider that, with new ways of communicating and accessing information, there are no more boundaries. "Private and business lives tend to get mixed up … You can damage the reputation of a company just by a few words posted on Twitter."

Delhalle pointed out that anything written on the internet can be used without the person responsible or their company knowing or being able to control it. He 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.

SICPA Management chief security officer Christian Aghroum also emphasised that people give a lot of information on social networks about what they are doing, where they are going, and so on, without realising that this can be useful to competitors.

Dennery said that companies now use social networking sites to communicate with all kinds of stakeholders, while their employees as private individuals also communicate on these sites. "We are in a world where information is open – but we have to take real care of the valuable information that produces our companies' income and gives our businesses a competitive edge," he warned.

"Information moves from one place to another in a second, so we have to be prepared to react quickly. It is not easy to be sure that you are informed of any leak and have a good action plan ready to preserve the reputation and value of your company. You have to consider crisis management." **SR**

online and offline, ACE insures progress

Property & Casualty | Accident & Health | Life

To address complex privacy issues, it takes the right people, a strong balance sheet, global capabilities, and a flexible approach. These are the strengths of ACE that allow us to offer a suite of products and services designed to address a broad range of technology, network security, privacy and data breach risks. We take on the responsibility of your risks so that you can take on the responsibility of making things happen. We call this *insuring progress.* Visit us at acegroup.com/eu

ACE® insuring progress®