StrategicRISK

GUIDE TO:

Cyber risk management

SPONSORED BY

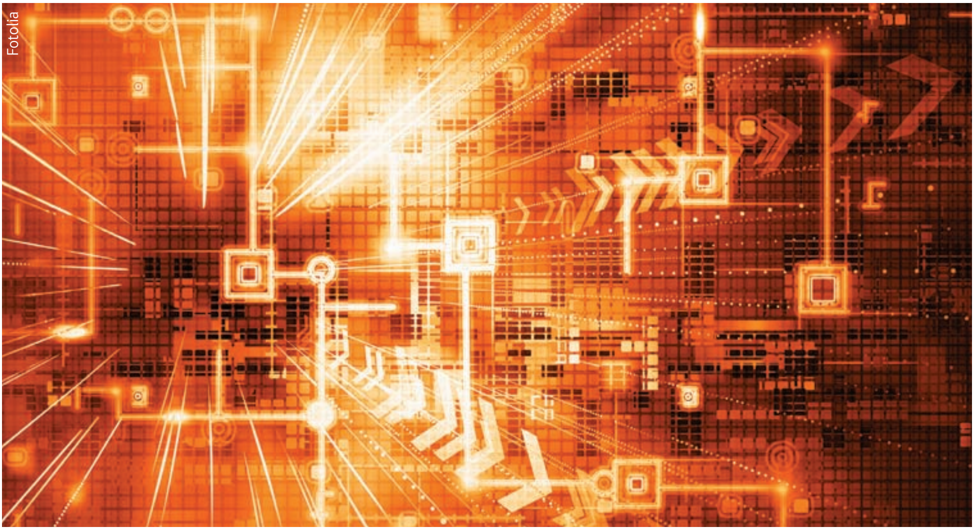
CHARTIS

Get CyberEdge.^sm Flexible solutions to handle cyber risk — and the chain reactions that follow.

When private information is compromised, the repercussions for your business can be serious and costly. That's why there's CyberEdge. From crisis management to legal investigations to identity restoration services, we can help manage and mitigate the effects of a breach, so you can stay focused on the bigger picture. Learn more at **www.chartisinsurance.com/uk/cyberedge**

CHARTIS®
Your world, insured

Chartis Europe Limited is authorised and regulated by the Financial Services Authority (FSA number 202628). This information can be checked by visiting the FSA website (www.fsa.gov.uk/Pages/register‹http://www.fsa.gov.uk/Pages/register›). Registered in England: company number 1486260. Registered address: The Chartis Building, 58 Fenchurch Street, London, EC3M 4AB.


Fotolia

2 | **Introduction**
As internet use balloons, cyber crime is also rising

4 | **European regulation**
A cyber crime centre and unified laws lead EU offensive

6 | **US regulation**
Data-protection laws are tough, but vary between states

8 | **Why it matters**
Regulatory action is expected to be stepped up

9 | **Case studies 1**
US healthcare firms' patient databases were accessed

10 | **Brokers' view**
Cyber cover is on the increase and becoming more affordable

14 | **Case studies 2**
Three companies' experiences of data breach

16 | **Elaine Heyworth**
Interview with the director of Heyworth Risk Consulting

20 | **Case studies 3**
Theft by former employees, and a website security flaw

22 | **Insurance market**
Cyber liability market is maturing

26 | **Threats**
Security breaches are not just down to criminal gangs and computer nerds

32 | **Top tips**
Seven ways to limit exposure

Editor Nathan Skinner
Editor-in-chief Sue Copeman
Market analyst Andrew Leslie
Group production editor Áine Kelly
Senior sub-editor Graeme Osborn
Sub-editor Simon Aldous
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

© Newsquest Specialist Media 2012

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

SPONSORED BY

CHARTIS

istockphoto.com

Moving up the agenda

Firms' appetite for protection against cyber risks is growing

IT'S A CLICHÉ TO say the internet is everywhere – but it's true. The numbers are simply staggering.

The Social Revolution on YouTube claims there are 9 billion connected devices worldwide at the moment and that will increase to 24 billion in the next eight years. The European Union claims that in 1995 just 1% of Europeans had access to a computer at home – by 2011, 73% had access to the internet at home.

And the numbers are only going to grow. Delivery may change but access and connectivity are not going away. Businesses rely on their systems to operate internally and to communicate with customers, all day every day.

So it is no wonder that cyber risks have moved up the agenda. The European Commission estimates that more than 1 million people worldwide are victims of cyber crime every day, while PwC reports global cyber security spending was expected to reach $60bn (£37bn) in 2011 and is forecast to grow at 10% every year during the next three to five years.

Its report claims the USA accounts for more than half of all security deals globally. This is no surprise, with the USA remaining a litigious society where

'Research suggests only 25% of firms are buying standalone cover. Potential for growth is massive'

privacy is closely guarded. However, new regulations being developed in the EU could soon enforce more stringent requirements across Europe too.

Suddenly, cyber liability is becoming a boardroom issue. Directors have a responsibility to address the risk or face the very real threat of angry shareholders and personal claims against them for dereliction of duties.

Cyber insurance has been available for a number of years but it too is evolving to meet the new challenges. More capacity is coming into the market and cover is adapting to match the demands of customers who need to shift cyber risks off their balance sheets.

Research by Chartis suggests 25% of firms purchase cover in the USA, where laws, litigation and knowledge are all conducive to high demand. In Europe the number would be less than 5%, according to Chartis, hence the scope for growth is huge. Many of the companies asked said they could afford to self-insure – brokers and insurers are seeing this attitude change as the regulatory requirements toughen up and companies realise the potential cost of a cyber attack.

According to the fifth annual US Cost of a Data Breach Study by the Poneman Institute, the cost of an event per record is rising at 9.2% every year in the USA and has already breached the $200 per customer record levels. Poneman also found the average total per-incident costs in 2009 were $6.75m, up from $6.65m in 2008. Consider that Sony had 77m customers affected by its data breach in April 2011 and the figures could be enormous. **SR**

THE NUMBERS

- Nine billion connected devices worldwide, predicted to rise to 24 billion by 2020
- More than 50% of the world's population is aged under 30
- If Facebook was a country it would be the third largest in the world
- 77 million customers were threatened by the Sony data breach
- Global cyber security spending was expected to reach $60bn in 2011
- It is forecast to grow 10% every year during the next three to five years
- Up to 600,000 Facebook accounts are blocked every day after hacking attempts
- More than 6.7 million distinct bot-infected computers were detected in 2009.

Europe fights back

The European Union has announced two major initiatives in the fight against cyber crime

Key points

01: All EU member states will now share the same set of rules on data protection

02: A European Cybercrime Centre is due to open in 2013

03: It will pool data gathered from industry, police and academics

BACK IN APRIL, THE EUROPEAN Commission proposed a comprehensive reform of the EU's 1995 data protection rules, strengthening online privacy rights.

The commission says: "A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3bn (£1.85m) a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe."

Key changes include:

- A single set of rules on data protection, valid across the EU
- Instead of the current obligation of all companies to notify all data protection activities to data protection supervisors, the regulation provides for increased responsibility and accountability for those processing personal data
- For example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours)
- Organisations will only have to deal with a single national data protection authority where they have their main establishment. Likewise, people can refer to the data protection authority in their country, even when data is processed by a company based outside the EU
- People will have easier access to their own data and be able to transfer personal data from one service provider to another more easily
- A 'right to be forgotten' will help people better manage data protection risks online
- EU rules must apply if personal data is handled abroad by companies that are active in the EU market
- Independent national data protection authorities will be strengthened and empowered to fine companies violating the rules, with penalties of up to €1m (£800,000) or up to 2% of the global annual turnover of a company.

The commission's proposals are being passed on to the European Parliament and EU member states for discussion. They will take effect two years after they have been adopted.

Cyber crime centre

In its second initiative, the commission has proposed a European Cybercrime Centre, within the European Police Office (Europol) in The Hague. It will be the European focal point in fighting cyber crime and will focus on organised illegal online activities.

A focus will be to protect social network profiles from e-crime infiltration and fight online identity theft

The EU experts will also work on preventing cyber crimes affecting e-banking and online booking activities. A focus will be to protect social network profiles from e-crime infiltration and will help the fight against online identity theft.

It will also focus on cyber crimes, such as online child sexual exploitation and cyber attacks affecting critical infrastructure and information systems.

The European centre will warn member states of major cyber crime threats, identifying organised cyber-criminal networks and prominent offenders in cyberspace. It will fuse information from open sources, private industry, police and academia and serve as a knowledge base for national police forces.

It will be able to respond to queries from cyber crime investigators, prosecutors and judges as well as the private sector on specific technical and forensic issues. Finally, the centre aims to become the natural partner for wider international partners and initiatives in the field of cyber crime.

The centre should start operations in January 2013. **SR**

istockphoto.com

KEY FACTS

- New rules could save European businesses around €2.3bn (£1.85bn) a year
- 17 years ago, fewer than 1% of Europeans used the internet
- By 2011, 73% of European households had internet access at home and in 2010, 36% were banking online
- 80% of young Europeans connect through social networks
- Approximately $8trn (€6.29trn) exchanges hands globally each year in e-commerce
- Worldwide, more than one million people become victims of cyber crime every day
- The cost of cyber crime could reach an overall total of US$388bn worldwide

istockphoto.com

Across the pond

The US government was widely reported to be unhappy with the European proposals to tighten data protection regulations across the member states. Below we take a look at the existing regime in the USA

Key points

01: Laws on data protection vary between US states but are typically tough

02: The latest rules on notification from California hand firms a huge burden

03: Any UK company that deals with the USA could be affected

THE USA HAS BEEN AHEAD OF THE curve in protecting its citizens against data breaches. Although there is no single federal statute on data protection, 46 of the states have developed their own regulations.

For any UK company that deals with the USA in any fashion, it is crucial to be aware of these rules – and of the penalties involved.

It is easier to list the states without such laws – Alabama, Kentucky, New Mexico and South Dakota. California was the first state to bring in new rules – and today these are still among the most stringent. Authorities in most states want to be kept informed of any breach that results in loss of personal data. Such data can include bank account or credit card details but also social security numbers and even driver's licence numbers.

Companies not only have to inform the state, but those affected: their customers. In January, California tightened its rules on notification once more and this is where it can get expensive.

California's Senate Bill 24 has established specific content for data breach notifications that must be sent to consumers. Any notification letter must include information on:

- A general description of the data breach
- What type of personal information was involved
- The date and time the breach occurred
- Whether notification was delayed due to a law enforcement investigation
- The toll-free telephone numbers and addresses of three credit bureaus, if the breach exposed social security numbers, driver's licenses or California identification card numbers

Entities that have been breached

must notify the Californian authorities if more than 500 people are affected by the breach. Credit watches are included in the remedial action to reassure consumers that their details are being protected. In an event like Sony's security breach in April 2011, when 77 million PlayStation Network customer details were released, the scale of remedial action becomes massive.

Credit card companies affected

A another example, Atlanta-based processor Global Payments announced in March that it had suffered "unauthorised access" into its system and had notified law enforcement and financial institutions.

Payment network operators MasterCard, Visa, American Express and Discover Financial Services confirmed they were affected, along with banks and other franchises.

Not only could Global Payments face large penalties, MasterCard shares fell 1.8% and Visa shares dropped 0.8% as the news broke – even though analysts said they were unlikely to face direct regulatory action.

Reports suggested some 10 million cardholders could be affected worldwide but the company moved swiftly to say the 1.5 million customers affected were all based in North America, with Track2 data stolen rather than personal details, and they were hopeful they had contained the breach. **SR**

WHY IT MATTERS

- What happens in the USA is often followed elsewhere
- Any company with US connections could be in breach
- Costs can escalate quickly to eye-watering figures.

The heat is on

Regulators worldwide are beginning to get to grips with cyber liabilities and there is a growing expectation that regulatory action will be stepped up, with penalties for companies that have failed to protect themselves adequately

istockphoto.com

US REGULATORY AUTHORITIES have been particularly zealous in pursuing companies experiencing data breaches and signs are emerging that organisations are taking this issue more seriously than before. The Ponemon Institute and PGP Corporation have been monitoring the cost of data breaches annually and recently published their findings for 2011. For the first time in seven years the cost of data breaches declined. Further, the organisational cost declined from $7.2m to $5.5m.

"This decline suggests that organisations represented in this study have improved their performance in both preparing for and responding to a data breach. As the findings reveal, more organisations are using data loss prevention technologies, fewer records are being lost in these breaches and there is less customer churn," says the report.

It has taken six costly years for US organisations to 'wise up', doubtless spurred by an increasing lack of tolerance of costly breaches from both shareholders and customers. European-based multinationals with operations in the USA should be well aware of the potential impact. Others are having that awareness driven home by EU and national regulation.

Another pointer for European businesses is the report by the Ponemon Institute that negligent insiders and malicious attacks are the main causes of data breach. In the 2011 study, for the first time malicious or criminal attacks accounted for more than a third of the total breaches reported. Since 2007, they also have been the most costly breaches. "Accordingly, organisations need to focus on processes, policies and technologies that address threats from the malicious insider or hacker," stresses the Institute. **SR**

Lessons to learn

In the USA, healthcare companies have often been the target of hackers, but these cases, reported by brokers Lockton, reveal that firms' own easily avoidable mistakes also increase the risk of data breach

Case study: Silicon Valley Eyecare Optometry and Contact Lenses

More than 40,000 patients were informed of a data breach after the firm was hit by burglars. The thieves stole the server containing the firm's patient database, including health information and personally identifiable financial information, such as dates of birth and social security numbers. The burglars broke in through a window and escaped with the server and a plasma TV; they were in and out within 50 seconds, according to on-site security cameras.

Lessons

Though the server was inside a locked room, it was likely to be visible from the window. The database was password protected, but unencrypted.

Database stewards need to plan better layers of both physical and logical security. This means storing servers in secure, concealed locations and encrypting data in the machines.

Case study: AvMed Health Plans

In February 2010, the firm went public with breach details from a late 2009 stolen laptop incident that it initially said exposed more than 200,000 records. By June, it had upped those figures to 1.2 million records. AvMed claimed the risk of fraudulent use of these records was low, but did not say whether the data was encrypted.

> *Consider whether sensitive information needs to be on laptops, in which case encryption is needed again*

Lessons

Laptops need not be out in the field to be easy targets for theft – these computers were in the office. A large number of data breach problems in health care can be pinned to lost and stolen laptops.

Consider whether such sensitive information needs to be on laptops and who requires access to it. Encryption is needed again if such information is on laptops at all. **SR**

The new buzzword

Cyber risk has rocketed up the agenda in the past year, becoming a hot topic at the US risk managers' conference

Key points

01: Human error, rather than cyber crime, is responsible for more than half of data breaches

02: The cost of cyber cover is becoming more affordable

03: The increasing practice of outsourcing data holdings is causing concern for reinsurers

CYBER RISK IS POPPING UP ON conference agendas worldwide like never before, according to Ben Beeson, a partner of the global technology and privacy practice at Lockton.

Beeson believes this reflects the growing awareness of the true risks faced by any company, whatever its size. And this is reflected again by the insurance markets. "You are seeing some insurers who have written cyber historically in the USA starting to turn their attention to the UK and Europe, which is a symptom of how the opportunity to sell cyber cover is changing," he says.

"Buyers are still very much concentrated in the USA," Beeson says. "But those in the UK and Europe with any kind of US exposure are waking up the risks. So far there is only around 30% penetration of insurance into the US market but that is increasing very fast. In terms of gross written premium, we are talking about $600m-$700m (€470m-£€550m), mainly written in the USA ,while capacity is centred in the USA and London, with a little from Bermuda."

There has been a "real sea change" in attitudes of Lloyd's syndicates, says Beeson, particularly from any of those writing US professional or financial institution lines of business – they all want to include some element of cyber cover. Buyers tend to be healthcare companies and financial institutions, which traditionally hold large amounts of customer data, but Beeson says retailers and hoteliers are also beginning to ask for cover.

"They are not comfortable keeping the risk on the balance sheet," says Beeson. "In the past 12 months it has become a boardroom risk – Sony has helped raise awareness but it was already evolving.

Firms forced to identify risks

"The icing on the cake was the Securities & Exchange Commission advice last year that listed firms should include information on cyber exposures. To do that firms need to understand their risk and once you have identified a risk it is hard to argue against shareholders who then want to know what you are doing to reduce that exposure."

Added to that, President Obama's proposed Consumer Privacy Bill is expected to push the issue yet higher on the agenda. This is not all being driven

Reuters

by the USA alone. Beeson says the European Commission's moves are significant and the next 12 months will be as busy as the last. "The combination of increasing capacity in the insurance market, more demand from insureds and the regulatory and legislative frameworks are adding to the overall picture," he says.

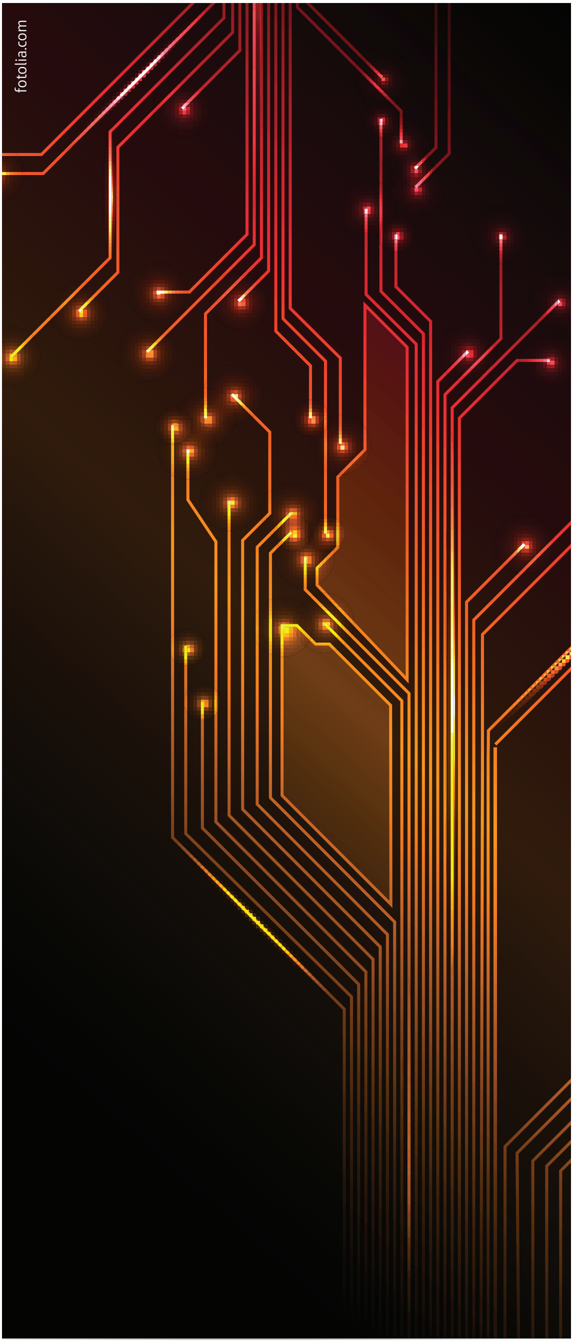
The role of human error

However, it is not likely to be all smooth sailing. Claims are increasing too – both in terms of frequency and cost. And there are some looming threats on the horizon. Lockton produced a report into cyber risks earlier this year.

One surprising fact highlighted by the report is that more than half (52%) of data breaches occur because of human error – lost computer devices and rogue employees stealing data, and just 32% are down to cyber criminals and hackers.

> *'It is virtually impossible for a company to protect its data from a breach'*
>
> **Ben Beeson** Lockton

"As the statistics reveal, the risks are both internal and external, which makes it virtually impossible for a company to protect its data from a breach. Instead, companies need to be prepared for a breach, understand the risks and assess


fotolia.com

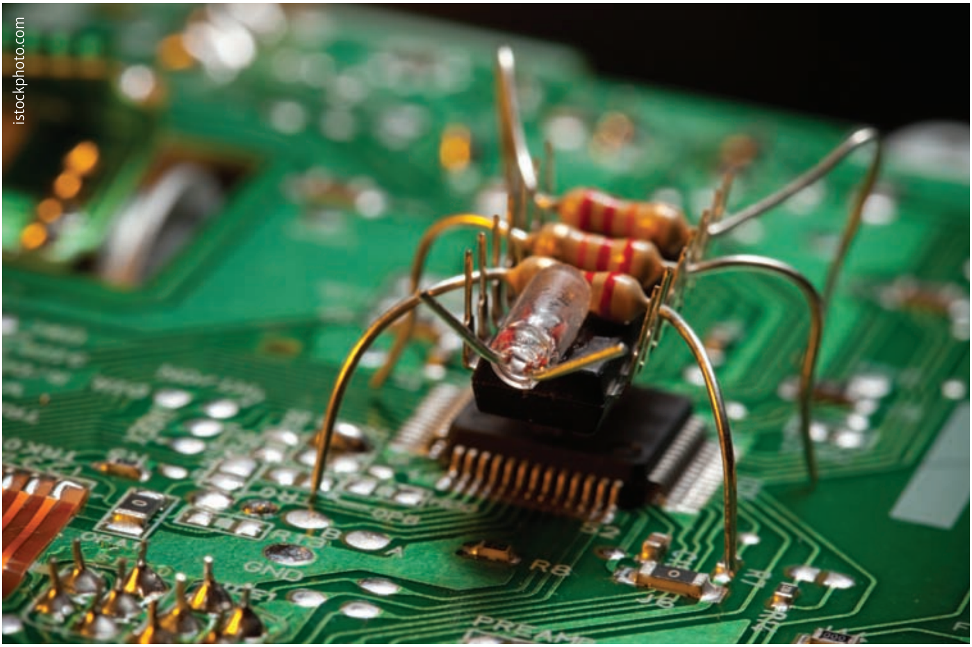
'Can you dare to put customer information into the hands of an outsource operation?'

Ben Beeson Lockton

how the financial impact can be minimised.

"Insurance not only provides much needed funds to deal with the immediate problems associated with a data breach, but it also gives access to experienced legal, IT and PR specialists who can help get a business back on track as quickly as possible. With technological developments happening daily, companies cannot afford to bury their heads in the sand when it comes to cyber crime and data risks."

And Beeson says companies need to be alive to the changing nature of cyber risks. Cloud computing, for example, is likely to become an increasing exposure. "Effectively companies are looking to outsource their data holdings. It may look like a good cost reduction to outsource this material at first glance but there could also be some real risks


istockphoto.com

attached and then the cost savings may not be as worthwhile.

"I could be accused of doom-mongering but companies need to think these implications through very carefully before taking any decision. Will you – or can you – dare to put consumer information into the hands of an outsource operation? More businesses will be doing it. It will be irresistible."

One breach, 10 claims

The good news, says Beeson, is that cyber insurance is designed to cover the risks. Slightly less good news for insurers is the danger of aggregation. If 10 companies all have cyber policies in place and, by chance, all use the same outsource provider and that outsource provider has a major breach, the insurer could be facing 10 major claims, triggered by the same event. Reinsurers are beginning to look at this very carefully, says Beeson, and "are getting nervous".

With more providers moving into the market and despite rising demand, the cost of cyber cover has been coming down to affordable levels. Insureds may face relatively high retention levels as insurers work to keep premium levels down – there are quite a lot of data breaches every year and, by maintaining high deductibles, insurers are there to help on the big claims.

As Beeson explains, "This is a market in its infancy. The UK and Europe have already learnt a lot from the USA but there is more to do. There are not enough actuarial figures as yet, particularly around risks such as cloud usage.

"Changing regulation and changing business models could catch some people out – and there could well be some major claims to come." **SR**

Cautionary tales

Any security system can only ever be as strong as its weakest link. Each connection to a third party exposes the company to new risks, as these firms discovered.

Key points

01: A breach at a US marketing firm affected Marks & Spencer UK customers

02: A gambling firm lost more than 3 million account details

03: Training needs to cover staff working from home with sensitive files

1) Epsilon

In March 2011, an incident was detected at US-based global marketing firm Epsilon where a subset of Epsilon clients' customer data was exposed by an unauthorised entry into the firm's email system.

At the time the company stressed "The information that was obtained was limited to email addresses and/or customer names only. A rigorous assessment determined that no other personal identifiable information associated with those names was at risk."

One of Epsilon's UK customers, Marks & Spencer (M&S), then had to warn its customers that their details may have been compromised.

Customers were warned that they might receive unsolicited emails but the firm stressed it did "take [their] privacy very seriously" and added it would "continue to work diligently to protect . . . personal information".

At the time the UK's Information Commissioners Office said it was investigating whether a breach of the UK's Data Protection Act had occurred. Other customers of Epsilon include names such as Hilton Hotels, Best Buy, Barclaycard US and Capital One.

2) Betfair

Online gambling firm Betfair admitted late last year that it had kept a major data breach from its customers. In 2010 more than 3.1 million account names with encrypted security questions, 2.9m usernames and nearly 90,000 account usernames with bank account details had been stolen.

Betfair also admitted it did not even know about the attack until two months later when a server at its Malta data centre crashed. It claimed it was unnecessary to inform customers because its security made the data unsafe for fraudulent activity.

When the breach was discovered, Betfair told the Serious Organised Crime Agency in the UK, together with the Australian Federal Police and the German authorities.

> *'The company did not know that data had been stolen until two months later when a server crashed'*

A social worker who took sensitive paperwork home was then burgled

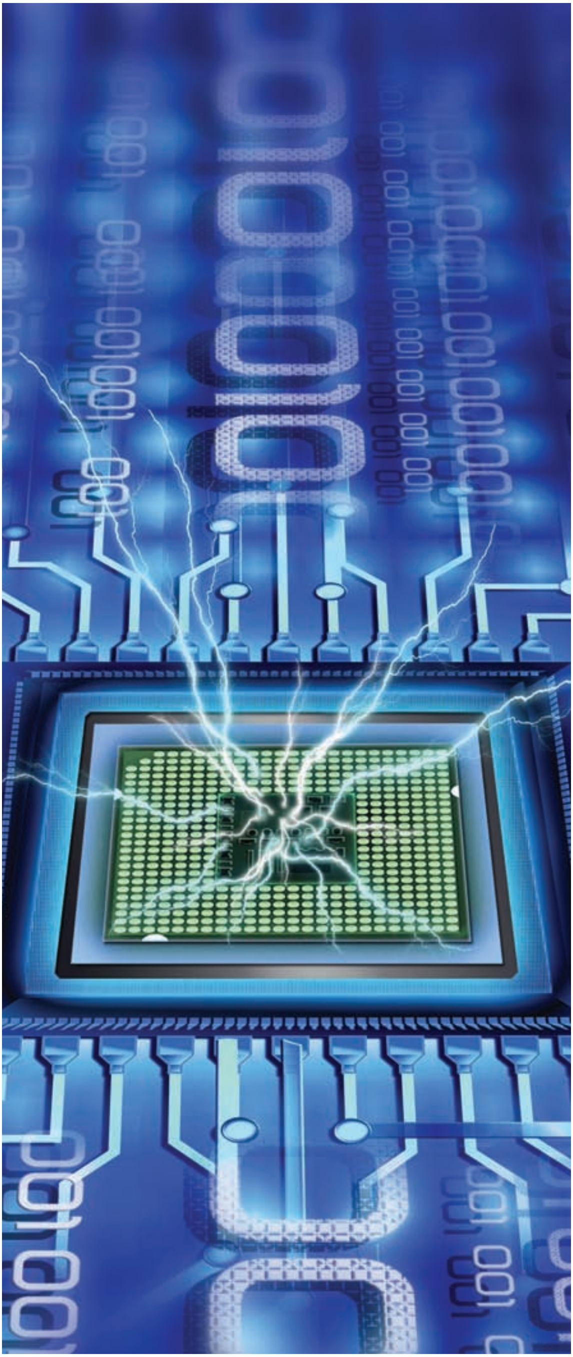
3) Leicestershire County Council

Earlier this year, the UK's Information Commissioner's Office reported that Leicestershire County Council had breached the Data Protection Act, following the theft of a briefcase containing sensitive personal data from a social worker's home.

The briefcase, containing documents to be used for initiating court proceedings and including sensitive personal data of 18 individuals, had been stolen from a social worker's house during a burglary. The social worker had asked for permission to take the reports home and this had been authorised by the relevant manager, in accordance with the council's procedures.

At the time of the incident, the employee's manager had received the relevant training, but the social worker had not. The authority had a policy in place but this did not relate to the handling of paper documents while working from home.

Since the breach, Leicestershire County Council has committed to amending policies to include detailed guidance relating to the security of paper documents while working from home, training staff on these amended policies, monitoring to ensure compliance, and implementing other security measures to ensure personal data is protected. **SR**



Be alert, be proactive, stay safe

Keeping abreast of the ever-changing risks from cyber exposure is all in a day's work for Elaine Heyworth, a director of Heyworth Risk Consulting. Below, she answers questions about how cyber risks are changing, how business leaders are taking the issue more seriously and why it affects everyone

fotolia.com

Key points

01: Rather than being organised criminals with an agenda, most hackers simply like a challenge

02: At present most risks are to reputation, so insurance to rebuild brands is useful

03: It is important to be proactive in identifying threats.

Do you think people have recognised the threat of a cyber breach?

Since cyber reached the UK government's national risk register a year ago, the issue has shot up in terms of general awareness across UK plc. However, cyber risks were already reaching the consciousness of many boards as high-profile targets were identified across the international media.

The first thing to do is separate the myth from the reality. People have an impression of an organised underground movement with a sophisticated plan to take big business down. And then there are the 17-year-old geeks sitting in their rooms and hacking into homeland security, who are only doing it because they can. They view hacking much as the 1980s generation viewed getting to the

THE THREATS

- Myth that your business is too small to be attacked
- Not understanding where your firm's weakness lies
- Not understanding social media
- Cloud computing

next level of Pac-Man. They regard it as a challenge to break down barriers and seem to have little awareness of the implications of what they are doing.

One of the biggest dangers for business is that companies don't understand what is happening to them or why.

What do you see as the biggest risk to business?

Sony in April 2011 was an interesting case. Someone stole all those details and then they did nothing with them. Ideally that would have been done by a 17-year-old supergeek who broke in as a challenge, taking on one of the world's biggest electronics firms for the hell of it.

The greatest risk so far has been to reputation. That's not to say the risk won't change, but so far it has been about managing the brand image once a breach becomes public.

In reality, how often do attacks happen?

When I was at T-Mobile, there were 35,000 attacks a day – and the figure went up significantly when we merged

fotolia.com

with Orange. We had layer upon layer of security. We were very aware of the risks and we worked hard to ensure we reduced the likelihood of any those attacks getting through.

I was lucky – I had a very good working relationship with our IT security head so I was able to ask him about the kinds of threat we faced and we could take the issues to the board together. Some hackers have been brought into the fold – poacher turned gamekeepers – and can provide some really useful insight.

What about insurance cover?

The biggest problem for us in finding insurance was that when we talked about liability, we didn't know what the liability actually was. If it was a loss of names and addresses, our insurance wouldn't pay out for the loss of names and addresses. If you had a case of insider cyber threat, then the insurers considered that to be fraud.

> *'When I was at T-Mobile, there were 35,000 attacks a day – and the figure went up when we merged with Orange'*

To be fair, insurers and brokers are working on it. But it is a struggle to identify the liabilities and therefore what you need to cover. There is a danger that some of the liabilities would be covered by other policies – for example, if someone hacked into a car manufacturer and reset the program so all the cars came out with three wheels. First, you would expect someone to spot the mistake before the cars left the factory

HEYWORTH IN BRIEF

Elaine is a director of Heyworth Risk Consultants, a non-executive director at RAFT Enterprises and a board member of the European Professional Women's Network

Her past roles have included head of risk management at Everything Everywhere, the company running two of the UK's most famous brands – T-Mobile (UK) and Orange (UK).

Owned jointly by Deutsche Telekom and France Telecom, Everything Everywhere is the UK's biggest communications company, with a combined customer base of more than 27 million people.

Before that, Elaine was head of environmental management, GRCB at Barclays Bank. She has also worked at Barclays Capital, Brooks McDonald, Olympus Capital Management and Goldman Sachs.

and, if they did go out and cause a crash, then the product or public liability policy would have stepped in. So where would the value of a cyber policy be? Losses at the moment are around reputation so policies that help with the costs of rebuilding an image may be more worthwhile.

A lot of companies buy a policy and think they have solved the problem. But as a risk manager you need to understand the threats you face so that you can work with your brokers and insurers to identify the right insurance. You can also reduce the threat and reduce your premiums. But you must be proactive.

What about risks for the future?

One of the dangers now – and for the future – is that small companies think they are too small to buy cyber insurance. They are at risk and should be thinking about it.

Cloud computing and privacy laws could become a real issue. If you put your data into cloud banks, where is it actually based? The USA has different rules to Europe, and Europe is different to Russia or to China. How can you build a global insurance programme with all these different rules? And how can you build a programme when you don't necessarily know which rules should apply?

I am a huge fan of social media and I think companies need to embrace it. It allows businesses to see what customers really think – and to find out what their employees are thinking too. Many firms ban employees from using it at work but I think that is the wrong approach. It is here to stay in some form or other. It is critical to tell you what is happening. Firms should not be afraid of it. **SR**

fotolia.com

Back to basics

While cloud computing and industrial espionage-style hacking are the hot topics, most data loss issues are more mundane. Companies might do well to concentrate on simple security measures, as these cases reveal

Key points

01: The courts are backing up the Information Commissioner's Office to curb data theft

02: Third-party web developers can introduce new risks

03: Data security needs to be re-tested after any changes to online applications

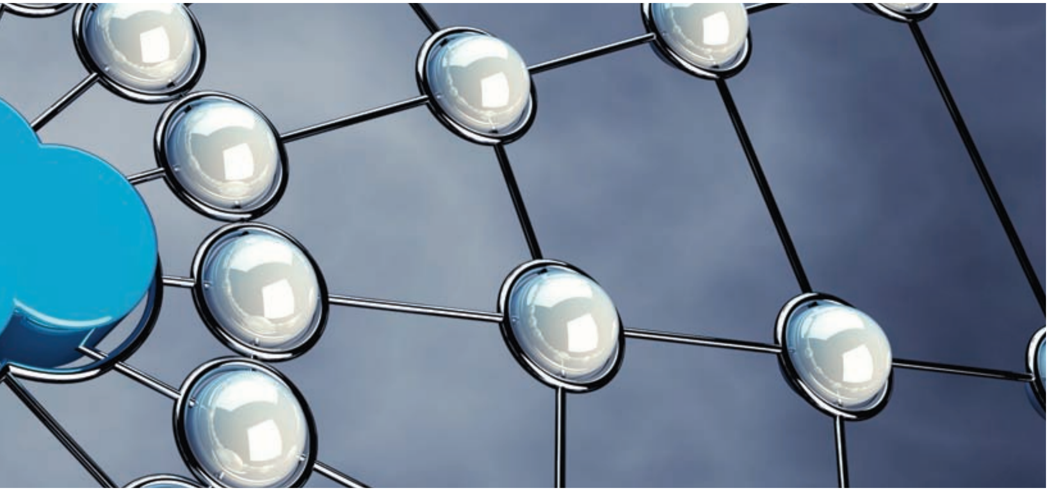
1) Customer data thieves made to pay £73,700

Two former employees of UK mobile operator T-Mobile who illegally stole and sold customer data from the company in 2008 were ordered to pay a total of £73,700 in fines and confiscation costs as part of a hearing at Chester Crown Court in June last year.

David Turley and Darren Hames pleaded guilty to offences under section 55 of the Data Protection Act (DPA) last year. The pair's offences were uncovered after T-Mobile identified an issue and turned the matter over to the Information Commissioner's Office (ICO) to help investigate how names, addresses, telephone numbers and customer contract end dates were being unlawfully passed on to third parties.

Information Commissioner Christopher Graham said in a statement: "The hearing marks the final chapter in an investigation that has exposed the criminals behind a mass illegal trade in lucrative mobile phone contract information. It also marks a new chapter of effective deterrents on data crime where the courts will act to recover the ill-gotten gains.

"Those who have regular access to thousands of customer details may think that attempts to use it for personal gain will go undetected. But this case shows that there is always an audit trail and my office will do everything in its power to uncover it. The lifestyle the pair gained from their criminal activities has been short-lived and I hope this case serves as a strong deterrent to others."



2) Website displayed personal data

Toshiba Information Systems (UK) breached the DPA after the personal details of 20 competition entrants were compromised by a security flaw on its website, the ICO revealed in April.

The ICO was informed by a member of the public in September last year that the personal details of individuals registered for an online competition on the company's website were accessible. These included names, addresses, dates of birth and contact information. The ICO found that the measures in place at the time of the incident were not sufficient to detect that a web design error had been made by a third-party developer.

Stephen Eckersley, the ICO's head of enforcement said at the time: "It is vital that, as ever-increasing amounts of our personal information are collected online, companies have the necessary safeguards in place to keep this information secure.

"We are pleased that Toshiba Information Systems (UK) have committed to ensuring that any changes to applications on their website are thoroughly tested by the developer and themselves, in order to keep the personal information they are collecting secure. We would urge other UK organisations with interactive websites to make sure they have suitable checks in place before collecting people's details online."

Toshiba Information Systems' commitment to keep the personal data it handles secure included the introduction of appropriate and proportionate data security testing on relevant web applications before they are launched. **SR**

> *'We would urge organisations with interactive websites to make sure they have suitable checks in place'*
>
> **Stephen Eckersley** ICO

fotolia.com

Seizing the moment

More players than ever are offering cyber liability insurance, and the market is maturing as insurers and insureds alike better understand the risks involved

UK AND EUROPEAN BUSINESS is set to grow, according to Chartis's vice-president of financial lines Europe, Shanil Williams, as the regulators toughen up and businesses recognise their growing exposure to cyber-related risks.

"It will become a hotter topic among risk managers," Williams says. "So far there has been a lot of talk but not much follow-up with their chequebooks. It is different in the US, where the laws and regulations have been more punitive, however tougher laws are on the horizon in Europe.

"Because a lot of the insurance business is written out of London, we do expect the UK to lead the way in this market, with Germany and France close behind. We are seeing more business in Spain too, thanks to an active Data Protection Agency. That said, we expect the demand curve to shift across the Continent including smaller countries like Slovakia and Hungary.

"To date, the majority of insureds have been companies with a turnover of more than €500m and have been quite industry specific; Telecoms, Healthcare, Retailers and Financial Institutions, because those firms hold more sensitive customer information. But we have also written business for companies with turnovers of €10m or less."

A lot of this market is driven by the USA. Chartis's vice-president of professional liability, Mark Camillo, explains: "We first launched this cover back in 1999. Then people were worried about web defacement or a loss of internet connection. It was a niche product that took off in a new direction when California introduced the first legislation in this area.

"Suddenly it became all about privacy, a loss of information and generally data protection. Companies started to realise that they would incur losses if they had to respond to a breach."

"They need cover for legal expenses and notification costs. Typically you can't send out a notification without adding something of value to the customer – card monitoring, for example."

KEY RISKS

The top three risks for organisations are:

- operational IT risks;
- customer information theft; and
- hacking.

Key points

01: Most UK and European firms are behind the USA in grasping the issues

02: First-response cover deals with the cost of notifications, while other liability cover kicks in later

03: There is enough capacity in the market to make premiums affordable

fotolia.com

> *'We want to step in early, not least because it helps reduce the cost of the overall claim'*
>
> **Shanil Williams** Chartis

Europe in footsteps of USA

US business is still building, but now the UK and Europe is expected to close the gap in coverage as momentum builds within the European Commission to enforce its new data protection proposals.

Williams says there is still a lot of education to be delivered in the UK and Europe. "Most stakeholders still don't appreciate the cost and complexity of handling a breach. If anyone has any US exposure, this cover is must-have, we are also increasingly seeing US clients asking for evidence of Cyber coverage when they contract with our Insured." The new proposed EU regulation will close the gap with the US legislation and companies need to be considering coverage now to be ready for mandatory notification for example."

When a breach happens, rapid-response is critical in managing the situation. We will work with our clients to ensure that we analyse the breach proactively, notify the affected people and provide critical crisis management services. We want to step in early – not least because it helps reduce the cost of the and the potential reputational damage," Williams adds.

His words are echoed by US-based Camillo, who stresses that the cost of failing to notify can be extremely high.

"Even where there are incidences involving third parties, we want to get on and start dealing with the incident, whether that be notifying the regulators or notifying customers.

CYBER LIABILITY: THE NUMBERS

- Gross written premium estimated at $600m-$700m.
- US market penetration heading to 30%.
- Most insureds are looking for €10m-€15m of cover.

"This helps keep the cost of the event down and we can worry about subrogation rights against the third party later."

Williams says risk managers should be evaluating both quantity and quality of capacity available in the market. Whilst there is reasonable appetite for this risk in the market it is important buyers ensure their primary coverage (at minimum) is adequate. Insureds should consider not only the third and first party coverage elements but also claims expertise, and ability for rapid response and to manage an event proactively.

The insurer finds most insured's are looking to buy around €10m-€15m of coverage. **SR**

A PRICE TO PAY

The cost of dealing with regulators is rising for companies suffering a data breach, however it may have been caused, as the case studies opposite reveal.

CASE STUDY ONE

What happened

An educational establishment in the USA accidentally made available on its website confidential information regarding about 42,000 students. A parent of one of the affected students filed a potential class action lawsuit alleging the insured violated her child's privacy rights and was negligent in failing to properly protect the student's privacy. In addition, the Federal Trade Commission launched an investigation to determine if the insured complied with the FTC Act, which prohibits misrepresentations about privacy practices.

Chartis payment

Paid out $250,000 (€195,000) in legal defence costs pursuant to the regulatory action sublimit of liability.

Comment

As Chartis's Mark Camillo explains: "We see claims coming from schools and colleges, often involving Google and Facebook. A pupil will Google their own name and up will pop a file from school, complete with confidential information. A file will have been added accidentally, but there are then costs associated with the legally required notifications."

CASE STUDY TWO

What happened

A printer wrongfully provided credit card information to a third party resulting in unauthorised transactions for its customers.

Executive liability payment

Paid more than $440,000 (€345,000) in legal defences.

Comment

Camillo explains: "The insured gave information to their printer, who shared it with another party.

"This kind of incident could be a problem for institutions such as banks, who may pass information to third parties like payment processors. The banks would have a duty to notify the authorities, as they would continue to have a duty of care for the information."

They're out to get you

The image of a group of radical hackers threatening to bring down the western world may be more the stuff of Hollywood fantasy, but threats to firms come in all shapes and sizes, from the 17-year-old nerd to large and organised criminal gangs. And sometimes the source of the problem can be much closer to home

Key points

01: Regulators expect financial institutions to have cyber crime policies

02: Encryption and bans on USBs, laptops and smartphones are among responses to insider threats

03: Four out of five people don't know who owns the data they put on social network sites

THE FIGURES SPEAK FOR themselves. Cyber crime has risen up the ranks over the last year to become the second most commonly reported economic crime affecting companies in the financial services sector after asset misappropriation, according to the latest findings from PwC's global economic crime survey.

And this is backed by figures from the International Chamber of Commerce, which claims that the global economic and social impacts of counterfeiting and piracy will reach $1.7 trillion (€1.3 trillion) by 2015 and put 2.5 million legitimate jobs at risk each year. While this is not an obvious form of cyber crime, counterfeiting starts with stealing designs, which can be done by hacking into the creator's system.

PwC believes cyber crime accounts for 38% of economic crime in the financial services sector, where half of those surveyed believe cyber crime has increased in the past year and some 45% of financial services respondents suffered frauds in the past 12 months.

PwC forensic services partner Andrew Clark says: "The rise in cyber crime is not so surprising given the sector holds large volumes of the type of data cyber criminals are interested in, and there is an established underground economy servicing the needs of the market for stolen and compromised data.

"Cyber crime puts the financial services sector's customers, brand and reputation at significant risk. Regulators are increasingly viewing cyber crime as a key area of focus, and financial institutions are expected to have appropriate systems and controls in place to fight this growing threat.."

Overlay this information with the figures from the European Commission that one million people are the victim of a hacking attack every day and the scale

of the problem becomes clear. But where do the threats come from?

Cloud concerns

Cloud technology allows businesses to store huge volumes of data offsite, in cyberspace. Risk managers, brokers and insurers are all concerned about this practise. Andy Bulgin, owner of AB Consulting, sums it up. "It is a great idea but it is fraught with difficulties. By putting your business documents on a cloud you are relying on someone else completely.

"Technology releases you in many ways but it can be a disaster. I had a major presentation on a laptop and travelled to Athens for the board meeting. Their system crashed and I was left just sitting there with nothing."

For the lawyers, risks associated with the cloud centre on jurisdiction. As DAC Beachcroft partner Patrick Hill explains: "The cloud is not designed to fit into our legal framework, which is based on jurisdiction and specific laws relating to that place – the cloud is just out there. One of its functions is that it straddles a number of jurisdictions around the globe."

There is also the question of aggregation – if insurers have a number of policyholders using the same cloud provider when a problem occurs, then the claim figures could mount extremely rapidly.

However, the insurers tend to be more bullish. They accept all these arguments but, as Chartis vice-president of professional liability Mark Camillo

> *'For many companies outsourcing on the cloud improves their security'*
>
> **Mark Camillo** Chartis

fotolia.com

explains: "For many companies outsourcing on the cloud actually improves their security. It can be very expensive for one firm to have all the necessary security in place, while a cloud provider can offer that automatically.

"I don't see it as a ticking time bomb. The cloud provider will want the best security because it is their reputation on the line. But the company should have its own passwords overlaying the cloud security, in reality adding another layer. Then even if the cloud gets hacked, the hacker still then needs each company's password."

Insider negligence

While people worry about the cloud and future developments, insurers, brokers and risk managers all say firms must never forget the risks closer to home. The Poneman Institute recently said that research indicates that: "Negligent insider breaches have decreased in number and cost, most likely resulting from training and awareness programmes having a positive effect on employees' sensitivity and awareness about the protection of personal information." Additionally, organisations have expanded their use of encryption.

Insider-related claims are still rolling in, however. Firms adopt a range of tactics to reduce the risks: some limit the number of people with access to certain information; some require several people to approve access at any time; some refuse to allow staff to use USB keys to

MORE WARNING NOTES

1) RETAIL ROGUE EMPLOYEE

What happened

Employee at a consumer reporting agency stole and sold personal information of more than three million customers.

Executive liability payment

Paid more than $5,100,000 (€3,995,000) in damages, more than $1m in legal defence costs and reimbursed the insured $1m for notification and credit monitoring costs. Source: Chartis

2) HEALTHCARE ROGUE EMPLOYEE

What happened

Rogue employee at a large medical provider stole and sold more than 40,000 patient records containing personally identifiable information.

Executive liability payment

Reimbursed the insured more than $700,000 for notification and credit monitoring costs. Source: Chartis

3) PAYMENT PROCESSOR HACKING

What happened

Hackers broke into the database of a credit card processor and accessed customers' personal data. A class action lawsuit alleged that the insured improperly stored unencrypted customer data and failed to maintain proper firewall protection.

Executive liability payment

Settled for $1,250,000 and paid more than $160,000 in defence costs. Source: Chartis

4) TECHNOLOGY/TELECOM HACKING

What happened

Unidentified individuals gained unauthorised access to a bank's ATM network operating systems and stole debit card information resulting in a total loss of $2,200,000 to bank customers. The resulting lawsuit alleged negligence for the fraudulent use of more than 400 debit cards that had previously been legitimately used at ATM locations in New York.

Executive liability payment

More than $2.4m in indemnity and defence costs. Source: Chartis

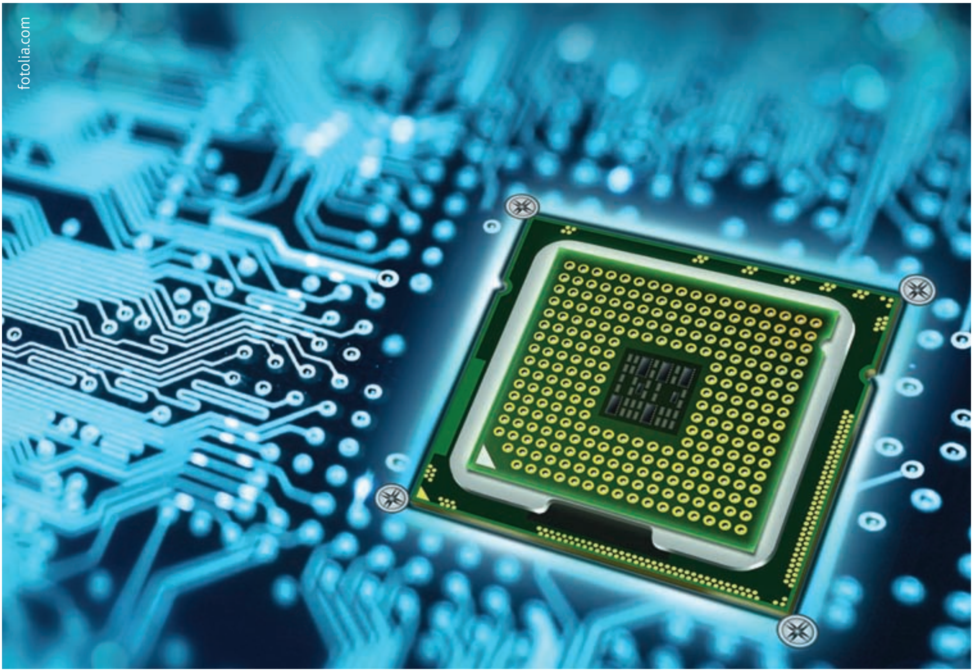
'The key is thinking about who has access to any data and how to keep control'

Patrick Hill DAC Beachcroft

carry information, do not have USB ports on office computers, or ban laptops.

The advent of smartphones has forced some call centres to collect staff phones at the start of every shift so that no information can be copied, and plenty of firms have clean desk policies so nothing is left in plain view.

But, as this example from Locktons shows, a back-to-basics approach might also be useful. The University of Texas Medical Branch was targeted by Katina Candrick, who allegedly used a stolen identity to gain employment at UTMB's medical biller, MedAssets, for the purpose of perpetrating fraud. She is suspected of unauthorised access and potential unauthorised use of up to



fotolia.com

2,400 UTMB patient records. Candrick was booked for many more ID theft charges around the USA, totalling more than $1m (€800,000) in losses.

Social media: 'Pandora's box'

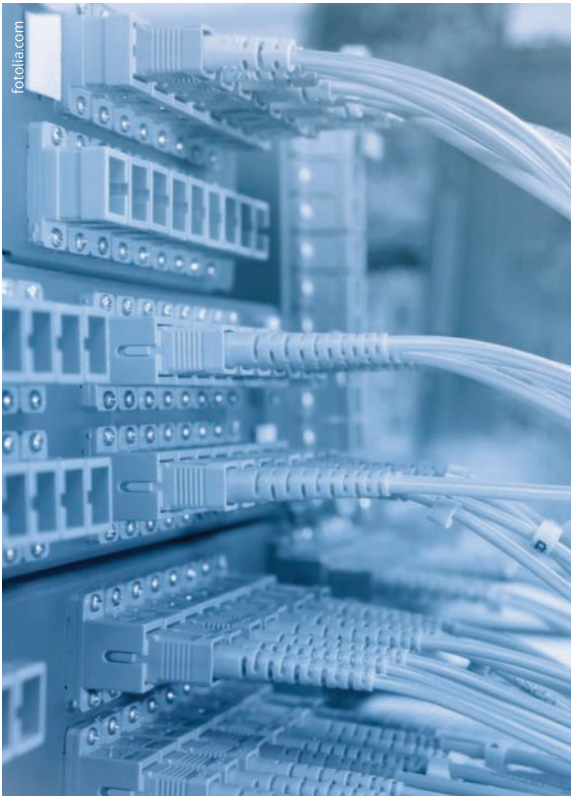
Social media has created another tier of anxiety. The EU is worried about the potential for abuse, saying that cybercriminals are targeting social media, with up to 600,000 Facebook accounts being blocked every day after various types of hacking attempts.

But as AB Consulting's Bulgin says: "Pandora's box was opened a long time ago." According to the Social Media Revolution on YouTube, Facebook tops Google weekly usage in the USA, and if Facebook was a country it would be third largest in the world. Fifty per cent of mobile internet traffic in the UK is for Facebook.

A report from Legal & General, *Digital Criminal 2012: CyberSafety,* reveals that almost half of people (49%) interviewed who use social networking sites are worried about the privacy and security of Facebook, rising from 46% of people in 2010.

In addition, and worryingly, 80% of those interviewed don't know who owns the data that they post on social network sites.

Companies are being encouraged to define their social media policy. The risk managers say options include limiting access to social media sites while staff are at work and having clear employment contracts dealing with behaviour on such sites.



fotolia.com

But as Elaine Heyworth of Heyworth Risk Consulting says: "Companies will be left behind if they don't embrace social media and make the most of the opportunities." The key is in balancing the risk with the opportunity and constantly being on guard against new threats.

Also, as Hill says: "The key is thinking about who has access to any data and to keep control of that.

"These are not really new risks, but it is the volume and speed at which companies can become embroiled in a breach which is challenging." **SR**

In case of emergency

The case studies in this guide should be enough to strike fear into the hearts of most risk managers. However, there are some key best-practice approaches that can help protect your business

> *'Very few single cyber-related events have the capacity to cause a global shock'*
>
> **OECD**

> *'There are significant and growing risks of localised misery and loss as a result of compromise of computer and telecommunications services'*
>
> **OECD**

Cyber risks may seem daunting. The speed at which an event may happen is frightening and the exposure for individual firms is escalating. But there are some simple precautions and strategies to take, which include:

1) Understand the risks and keep updated with developments.
2) Stay friends with the IT department. Work with IT teams to understand the risk and to pass on those messages to the board.
3) Keep the board updated. Board members have growing responsibilities in this area. Make sure they understand the risks and hear about solutions.
4) Work with HR and IT teams to develop clear IT security policies for staff. Make sure new staff are trained and that existing staff are kept up-to-date.
5) Work with HR, marketing and anyone else involved in developing a social media strategy, both for work purposes and expected behaviour beyond the workplace.
6) Work with insurance brokers and insurers in understanding the risks and reducing your exposure.
7) Have emergency plans in place should a major breach occur. This should cover both physical threat and privacy issues, as well as damage to reputation. **SR**

Get CyberEdge.℠
Flexible solutions to handle cyber risk — and the chain reactions that follow.

When private information is compromised, the repercussions for your business can be serious and costly. That's why there's CyberEdge. From crisis management to legal investigations to identity restoration services, we can help manage and mitigate the effects of a breach, so you can stay focused on the bigger picture. Learn more at **www.chartisinsurance.com/uk/cyberedge**

CHARTIS®
Your world, insured

Chartis Europe Limited is authorised and regulated by the Financial Services Authority (FSA number 202628). This information can be checked by visiting the FSA website (www.fsa.gov.uk/Pages/register‹http://www.fsa.gov.uk/Pages/register›). Registered in England: company number 1486260. Registered address: The Chartis Building, 58 Fenchurch Street, London, EC3M 4AB.