CYBERSECURITY

FINANCIAL TIMES **SPECIAL REPORT** | Tuesday November 1 2011

Inside
Targeted attacks are here to stay, writes Maija Palmer
Page 4

www.ft.com/cybersecurity-november-2011 | twitter.com/ftreports

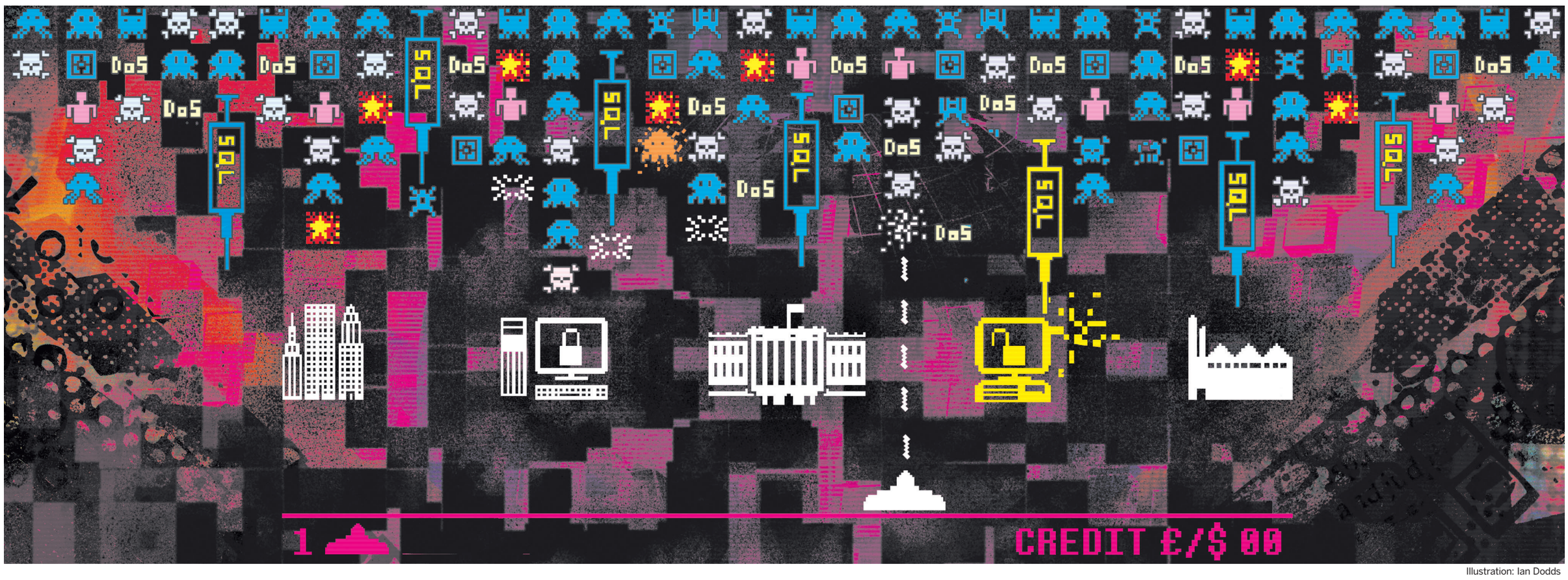


Illustration: Ian Dodds

A war marked by fatalism and denial

It is possible to win battles easily and cheaply, explains **Joseph Menn**

While large companies around the world realise that cybersecurity weaknesses are a growing threat, they are not increasing spending to meet the challenge, according to recent surveys.

In a PwC poll of thousands of executives, just over half the respondents expected their companies to spend more next year on technology security, just as they had the year before.

Yet the confidence of those information technology executives and PwC clients in their organisations' defences has sunk to the lowest point since the survey began six years ago.

The apparent contradiction raises troubling questions about the state of the technology, corporate governance, and the ability of company leaders to act in a complex and evolving arena without a short-term crisis or similar motivation.

The apparent paralysis has deep but distinct roots. "There is fatalism, and there is complacency, and there is denial," said Sir Kevin Tebbit, former permanent under secretary of state at the UK ministry of defence and, before that, director of GCHQ, the nation's signals intelligence agency.

In October, Sir Kevin spoke at a conference in London promoting links between cybersecurity and the wellbeing of businesses and the broad economy, and showing how good practice can be a competitive advantage. A conference convened this week by William Hague, the UK foreign secretary, expected to draw attendees from 60 countries, will tackle that issue and others.

Such efforts can become an uphill battle. In part, that is because senior executives feel the fight is hopeless, consultants say.

Big defence contractors such as Boeing, ManTech, and Northrop Grumman have all been compromised in the past two years. So, too, have leading security companies, including top security software vendor Symantec and EMC-owned RSA, the leading maker of tokens to authenticate computer users.

The more educated many professionals become about how such high-end attacks are carried out, the more alarmed they become.

Often attributed to hackers working with the military or other government agencies in China, those attacks are often described as "advanced persistent threats" (APTs).

They can combine tricking an employee by posing convincingly as a colleague, with programs that take advantage of vulnerabilities in software, known as zero-day exploits.

Such campaigns were initially aimed at government agencies and are moving to embrace military suppliers and more recently other industries, according to Mandiant, a US firm that has conducted investigations on behalf of many of the highest-profile victims, including Google.

"Mandiant has seen a growing number of commercial entities compromised," the company wrote recently in a trends report, noting that it has been involved in cases in energy, banking, mining, automotive and even the hospitality industry.

Executives have taken note, telling PwC in large numbers that APTs are the driving force behind their defensive spending.

Unfortunately, only 16 per cent of them say they have the right policies in place to ward off such threats. Some key capabilities, from alert-management processes to awareness training, are actually in declining use.

"Companies wonder: 'Is there really anything I can do about it?'" says Henry Harrison, cybersecurity director at BAE Systems' UK-based Detica unit. "But management is at least having those conversations."

> Frequent reports of breaches at big companies have reduced the stigma attached to victims

The fatalism is a mistake in the view of Mr Harrison and many others. Companies can raise the odds against the worst kind of data-loss – trade secrets, masses of customers' information, and the like – if they put in the effort.

Among other things, it requires redefining what winning is, says Mandiant. The bad guys are going to get in, but they can be stopped from getting data out. In addition, most hacking attacks are not carried out by evil geniuses, but by young criminals using readily available tools and scanning for holes in the system that allow them to gain access.

The $170m attack on Sony and others this year used a technique called SQL injection, which can be prevented cheaply.

A recent analysis by Imperva, a security firm, of internet conversations on one popular hacking forum found SQL attacks were the second most popular topic of discussions, after denial-of-service-attacks, which need even less skill.

Indeed, fewer than 1 per cent of the infections Microsoft detects are via security holes breached by zero-day events, the software group said last month.

Republicans in the US House of Representatives, who are proposing broad legislation to improve the country's security, said in October 90 per cent of attacks could be avoided with "good hygiene".

If executives know that, why are they not insisting on good practices?

It may be the rewards for success and the penalties for failure are too low. Because chief executives expect security teams to avert catastrophes, the absence of a successful attack is rarely grounds for a bonus.

And the increasingly common reports of breaches at big companies have reduced the stigma attached to victims of successful attacks and the security figures who work there. The danger is that the very frequency of such reports could lead to complacency.

Even when the attacks are serious, the damage is often unclear. The breaches may not be reported to authorities or to customers, so not immediately harming the brand.

They may prompt little more than security enhancements that fall within a reasonable overall technology budget and are unlikely to lead to a firing

The potential exists for outright and very public disaster, but it is still small enough that the third prong of Sir Kevin's problem statement comes in: denial.

It is human nature to avoid hard work aimed at avoiding something that has only a small chance of a career-shortening bad outcome, veterans in the industry say. A few things would help break out of the stasis many politicians, defence leaders and security professionals say is putting the economy at risk.

One would be simpler choices, such as the option of more affordable and comprehensive cyber-insurance.

Something that made it easier to sort through the morass of marketing hype around security software would also be a boon.

Some of the biggest all-purpose technology providers, including Hewlett-Packard and Dell, have bought security firms in the past year and might be on the road to giving thorough protection as a service.

But the attempted fix that is likely to arrive the soonest is increased mandatory disclosure.

In a lengthy public statement from its staff released in mid-October after pressure from members of Congress, the US Securities and Exchange Commission said cyberattacks that could be material should be revealed to shareholders of publicly traded companies.

"Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber-incidents, a number of disclosure requirements may impose an obligation on registrants," the staff wrote.

Potentially material costs could include increased security spending, reputation damage and lost revenue.

Since the new guidance also encompasses disclosures of risk factors, John Reed Stark, a former SEC internet enforcement specialist, says he expects the number of the largest 500 companies reporting cyber-threats to soar from today's handful.

"There isn't a regulated entity out there that on any given day isn't subject to attack," says Mr Stark, who heads the Washington office of Stroz Freidberg, a digital forensics firm. "It's certainly going to be a large number that are vulnerable to this."

The hope of those who pushed for the SEC action is that it will make cyber issues command the attention of chief executives, as well as the public. That could lead to more strategic thinking on the issue, both inside corporate hacking targets and at large.

Inside

Cybersecurity

Mitsubishi Heavy Industries was reported to have been infected with malware that affected equipment at its Tokyo headquarters and its manufacturing facilities Getty

A huge challenge from China, Russia and organised crime

Security

James Blitz considers what can be done about advanced persistent threats

What can security companies do to prevent governments and large corporations being attacked by "advanced persistent threats" in cyberspace?

This is one of the topics that is most hotly debated by cybersecurity experts. Advanced persistent threats – or APTs – are attacks at the most sophisticated end of cybercrime activity. They are aimed at extracting high-value intellectual property from governments or corporations. They can do immense damage to the targeted organisation – and they can be hugely difficult to stop.

Over the past few years, there have been a growing number of such assaults. The Stuxnet worm launched against Iran's nuclear programme is the most famous APT, doing tangible – though not permanent – damage to Tehran's uranium enrichment facility at Natanz.

Stuxnet is widely assume to be a worm developed by the US and Israeli governments, though neither has confirmed this.

More generally, APTs have been used as a potentially powerful weapon in industrial espionage.

In March, an information security breach at RSA, a leading US-based security company, led to reported attempts to steal information from US defence company Lockheed Martin, which, the company said, were unsuccessful.

In September, there were reports that Mitsubishi Heavy Industries had found that equipment at its Tokyo headquarters and its manufacturing facilities was infected with malware.

The question of who carries out these threats is a matter of much debate. The strong assumption on the part of western security agencies is that Chinese and Russian governments – and their proxies – are significant forces. "The Chinese are notable for the sheer volume of what they do," says one leading European security official. "The Russians are less active, but what they do is very sophisticated."

Another security official is more blunt: "APT is basically a synonym for China."

Others, meanwhile, insist it is not just nation states that are responsible for this kind of sophisticated espionage. According to John Skipper, a cybersecurity expert at UK-based PA Consulting Group, groups involved in organised crime have been deploying APTs.

But it is hard to obtain an accurate picture of how many such attacks are taking place. As Henry Harrison, technical director of Detica, a technology consulting firm owned by BAE Systems, puts it: "The reality is that companies don't like to talk about being attacked, so a lot doesn't get reported."

> 'The Chinese are notable for the sheer volume of what they do. The Russians are less active but very sophisticated'

However, Sam Curry, chief technologist at RSA, says a lot can be done to defend systems against such attacks. "Right now, the trend is for defences to worsen while opponents become more effective. We are in a constant state of infrastructure compromise. But this does not have to mean organisations need to live in a constant state of risk."

One important point made by leading security companies is that organisations need to have systems in place that tell them when these attacks are taking place. "The starting point for companies is that they need to know they will never have 100 per cent defence against APTs," says Mr Harrison. "The key, therefore, is to have mechanisms in place that recognise when your system has been compromised and take action accordingly.

"The time lag between initial compromise of a computer system and the moment when an attacker finds the information he is looking for can be a number of weeks. The challenge is to terminate the attack in that critical window."

Companies also need to be aware of a wide range of issues as they plan defences. "People need to build protection right across their businesses," says Mr Skipper of PA Consulting. "They need to monitor unusual behaviour going on around them. They need to keep a close eye on staff. Many of the most successful APTs ultimately have their origins in a human element inside the target organisation."

Mr Curry believes that companies need a new range of tools, combined in fresh ways and taking advantage of technological advance, to tackle APTs.

"People need to go back to the basics," he says: "Limit access, harden systems and simplify the environment rather than making it more complex. They also need to start looking at security and network analysis.

"Situational awareness and orientation are vital. Very often the question is who might target you and your customers and partners and why, rather than how would they achieve their aims."

In the long run, the challenges for companies will be huge. As Mr Curry puts it, they will have to do a lot of lateral thinking if they are to stop APTs getting through. "People need to stop preparing for the last war," he says. "Contemporary threats can completely bypass static, traditional defences. Today's smart APTs have a stockpile of never-before-seen tools that they will use against you."

The trade-off between risk and cost

Insurance

Premiums are high but will fall over time, writes **Maija Palmer**

Insuring against cyber-attack has not been high on the agenda for companies up to now. But the attack on Sony this year served as a wake-up call.

The attack exposed the details of 100m Sony PlayStation customers and is expected to cost the Japanese electronics company $182m this year, and it is facing 55 class action lawsuits. Worse yet, Zurich American, one of Sony's insurers, is arguing in court the insurance it wrote does not cover digital attacks.

Courts are increasingly deciding general insurance cover does not extend to cyber-incidents, says Steve DeGeorge, partner at Robinson Bradshaw, the law firm. The US Court of Appeals in North and South Carolina, for example, ruled this year that insurance covering tangible property does not extend to electronic data.

"There is a perception that if you have commercial general liability insurance, you will be covered," he says. "But this is a very risky strategy."

In addition to well-publicised attacks such as Sony's, security experts say thousands of other attacks on businesses go unreported. Experts believe most companies will have suffered some kind of internet attack.

A UK government study this year indicated internet crime costs businesses £21bn a year, with £9.2bn being intellectual property theft and £7.6bn industrial espionage.

The cyber-insurance market is growing, with Lloyds, the insurance company, estimating it to be now worth $600m a year, from $450m two years ago.

However, only a quarter of companies in the UK have insurance against cybercrime, in spite of more than half seeing a rise in threat levels over the past year, according to a study by KPMG.

Just 27 per cent of UK businesses have insurance against data loss and a policy covering them for business interruption by hackers. Only 22 per cent have insurance to cover the potential large legal costs associated with an ecrime incident.

Mr DeGeorge estimates that just 15 per cent of US publicly traded companies have cybercrime insurance. In some industries, such as healthcare and banking, however, this is beginning to change.

Kim Holmes, healthcare product manager for the Chubb group of insurance companies, says there has been a large rise in interest from healthcare companies, after the US brought in the High Tech Act in 2009, tightening protection of private health records.

Under this law, companies can be fined up to $1.5m if such data are exposed.

Class action lawsuits, such as the $20m suit being brought against Stanford Hospital for loss of data, are making the issue very real for this sector.

"It is now talked about as a when – not an if – scenario," Ms Holmes says. "In healthcare, folks are actually listening because the High Tech law is clearly here today. Other industry sectors, however, are not under the same government scrutiny and so there is not the same urgency."

Cost is one of the main factors stopping companies taking out cyber-insurance. A typical premium might be $5,000 for coverage of $1m, according to Mr DeGeorge. "We are in a very difficult economy and businesses don't have the appetite for additional spending. Companies think they have already invested a lot in their internal security and may feel that buying insurance on top of that will be hard to justify to shareholders," he says.

Part of the reason for the high costs is that underwriters have difficulty assessing the threat.

"People providing cyber-insurance are flying blind, because the threats are so difficult to predict," says Malcolm Marshall, head of UK information security for KPMG.

"Cyber-insurance has only been around for about 10 years, in a 300-year-old insurance industry. There is no reliable actuarial data to help inform underwriters' pricing."

Mr DeGeorge says: "When any insurance product comes to market, there is always a period of years when issues come to the fore and are fought out in the courts."

> 'People providing cyber-insurance are flying blind, because threats are so difficult to predict'

Costs may come down. Some 20 years ago, when pollution and environmental liability insurance first came on to the market, it was very expensive because underwriters did not know how to price the risk. Now costs have come down considerably.

"I think we will see the same development in cybercrime insurance," says Mr DeGeorge.

Especially if more companies in a variety of sectors are obliged to report cyberattacks, a body of data will develop.

In the meantime, companies can obtain lower insurance quotes by getting internal security as tight as possible, and monitoring the threats they want to be protected from.

"A policy written in 2011 may be obsolete in a couple of years, because this area is developing so fast. Something could happen that is not covered, because it was unimagined a few years earlier," Mr DeGeorge warns.

"It really is the case that, every year when the policy comes up for renewal, you should look at how the world has changed and how the company's requirements may have changed with it."

Businesses told to reveal true scale of losses

SEC filings

Fresh guidelines are likely to be a burden for US companies, writes **Joseph Menn**

One of the difficulties in fighting cybercrime is the uncertainty about how much it costs companies, countries and individuals.

Without this information, it is hard to determine what should be spent to combat the problem – let alone who should be spending the money and on what.

For annual global losses, estimates range from below $100bn to as much as $1,000bn, an industry report's ballpark figure that has been cited by Barack Obama, the US president.

This figure includes lost intellectual property, which could be worth far more to the inventor than to the thief, but it does not include national security, which is hard to put a price on.

But many more professionals are about to start making educated guesses about the costs to specific companies, potentially helping both top executives and society as a whole understand what they are up against.

On October 13, the staff of the US Securities and Exchange Commission issued extensive guidelines to companies that are publicly traded in the country, spelling out when and how both past cybersecurity breaches and the risk of future ones should be disclosed in regulatory filings viewable by anyone.

That will prompt many, if not all, of the several hundred largest companies to start opening up about what they have lost and what they stand to lose, says John Reed Stark, a former SEC official and now managing director of Stroz Friedberg, a digital security firm.

Even if companies do not leap to adhere to the agency's mandate that they avoid vague language – such as a retailer warning that all industry databases of customer data could theoretically be targets – laws that reward whistleblowers will encourage employees and others to tip off the SEC about serious breaches.

"The SEC has issued an all-points bulletin to any whistleblower out there: 'Let us know and you may be able to get up to 30 per cent of whatever fine we levy'," Mr Stark says.

"It is terrific that the SEC has come in, but it is going to be a tremendous burden for public companies," he adds.

Companies will now have to cover specific security issues in the "risk factors" section of their regular filings. System compromises that have a material impact on results or financial conditions, or that are likely to do so, must be reported in management discussions of recent performance.

They could even potentially be included in so-called 8K filings, which describe special events.

The combined disclosures should "provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant", the SEC wrote, adding that reputational damage, loss of customers and strategic trade secrets would all be factors to consider.

Though a fair number of companies have mentioned hacking threats in passing, thus far very few have disclosed actual breaches and their financial consequence.

Intel, the US microchip group, and Google did so early last year, after the internet company announced that hackers based in China had tried to gain access to the accounts of political dissidents.

However, these companies have not put a dollar value on the impact.

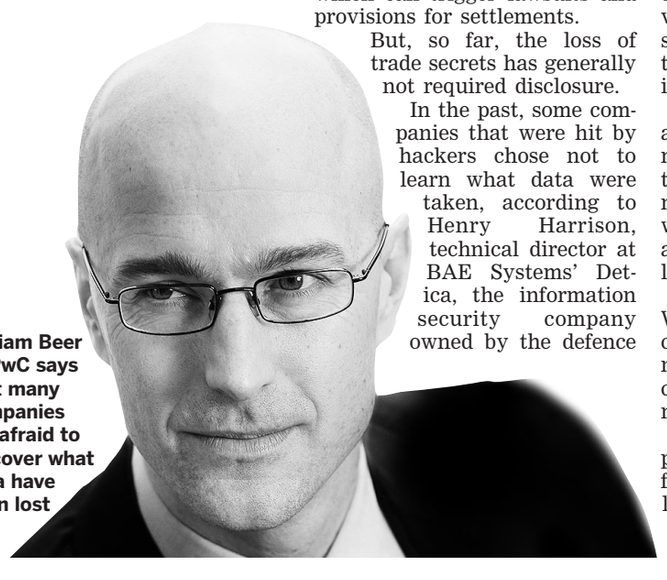
As regards extended outages and credit card thefts, some disclosures have been more precise. Sony, the consumer electronics group, said it stood to lose about $170m after its online gaming networks were attacked repeatedly this year.

TJX, the US retail group that owns TK Maxx, and Heartland Payment Systems, a payment processing company, said that being victims in some of the largest credit and debit card number thefts yet reported had cost them more than $250m and $140m respectively.

US laws force companies to warn customers when they lose sensitive data about them, which can trigger lawsuits and provisions for settlements.

But, so far, the loss of trade secrets has generally not required disclosure.

In the past, some companies that were hit by hackers chose not to learn what data were taken, according to Henry Harrison, technical director at BAE Systems' Detica, the information security company owned by the defence equipment group. This is confirmed by veteran contract investigators in the US.



William Beer of PwC says that many companies are afraid to discover what data have been lost

William Beer, a director of the cybersecurity practice at PwC, the professional services firm, comments: "It is a bit of a Pandora's box. You could discover some pretty nasty problems, so the easy option is to keep the lid shut."

However, a policy of deliberate ignorance might be untenable in the wake of the SEC policy.

If companies start to admit dire events – such as software vendors disclosing the loss of source code for key programs – they could face stock sell-offs by investors.

Security veterans disagree about how often such things might occur, but say that anything beyond a few public statements about events on this scale will encourage a public debate and could force stalled security laws through legislatures.

Richard Clarke, the former White House cybersecurity chief, says more disclosure is not only fairer to investors, but could galvanise Congress into more helpful action.

"If you are a company and 90 per cent of your revenue comes from three drugs and the formulas are gone and they are being knocked off in India, what, really, is your worth?"

Contributors

Joseph Menn
Technology Correspondent

Maija Palmer
Technology Correspondent

Chris Nuttall
Technology Correspondent

Alan Rappeport
US Consumer Correspondent

James Blitz
Defence and Diplomatic Editor

Stephen Pritchard
FT Contributor

Adam Jezard
Commissioning Editor

Steven Bird
Designer

Andy Mears
Picture Editor

For advertising details, contact:
Liam Sweeney
+44 (0)20 7873 4148
Fax +44 (0)20 7873 4006
Email: liam.sweeney@ft.com, or your usual representative

All FT Reports are available on FT.com.
Go to: **www.ft.com/reports**

Follow us on twitter at **www.twitter.com/ft.reports**

All editorial content in this supplement is produced by the FT.

The cloud still has a silver lining but it may be costly

Data protection

Stephen Pritchard looks at why higher levels of defence need to be provided

Not too long ago, any IT director would have been dismissed as irrational – if not dismissed from the business altogether – for proposing that critical company data be put on a shared computer, accessed via the internet.

Today, the IT industry is exhorting businesses to do just that, through cloud computing.

Some vendors are even bypassing the IT department, and going straight to business units to sell them services such as sales force automation, or customer relationship management. These services are invariably delivered via the cloud.

And by no means all cloud services operate with enterprise-grade security; many have origins in consumer services designed to be cheap and easy to use.

Neil Campbell, general manager for security at Dimension Data, an IT services vendor, cautions: "If it is a consumer service, you would expect basic security controls but not a high level approach to security."

In part, this is a function of how cloud computing works. In order to be cost-effective, providers have to take a "one size fits all" approach to their business, including security. By comparison, much enterprise IT would more closely resemble bespoke tailoring.

William Beer, a director in the information security practice at PwC, the processional services firm, explains: "Vendors have focused on the flexibility and cost-saving elements of the cloud and have locked down the contracts very tightly. It's a service that they want to be replicable."

That, though, says Mr Beer, means businesses moving to the cloud will have less control over their operating environment, including their security, than with traditional in-house IT or outsourcing models.

However, cloud service vendors are changing their business models to suit the demands of security-conscious customers. As well as private clouds, set up for one company, and community or "trusted" clouds, created to serve the needs of a group of related firms or government departments, generalist cloud service providers are also bolstering security.

"Amazon and Google are moving into the business space through enterprise levels of encryption and service," says Rupert Chapman, an IT security specialist at PA Consulting. "If it is a private or trusted cloud it may be able to deliver services that are as good as or better than in your own data centres."

"Whether there's a higher level of security will depend on the size of the organisation procuring cloud services," says Peter Allwood, a manager for information security and risk

'A trusted cloud may be able to deliver services as good as your own,' says Rupert Chapman

at Deloitte, the consultancy.

He adds: "SMEs may not have enterprise security infrastructure. Cloud was invented for SMEs, so they can take advantage of enterprise security measures the cloud provider has developed."

But larger organisations should not assume that enterprise-grade security will come with a consumer or small business cloud service. Depending on the cloud provider, upgrading security may be difficult. Bespoke or highly customised cloud services, usually created by large IT systems integrators, will be more accommodating.

PA's Mr Chapman says: "We have shown clients the security from a [customised] cloud service, and the conclusion was that because it was part of the provider's unique selling point, they could do it better than the enterprise, with more money, and more focus."

And, with high-level IT skills – and IT security skills in particular – in short supply in most western economies, moving services to the cloud actually boosts security. This is especially true for short-term or proof of concept projects, where cloud computing's flexibility is already very attractive.

But concerns remain about putting sensitive information and data into the cloud. Businesses need to know where their data are stored. EU businesses have legal restrictions on hosting personal data outside the Community. This has led larger cloud service providers to set up data centres within Europe. But businesses still need to ensure security and data privacy practices are integrated with those of cloud providers.

A more complex issue is whether cloud service providers are, themselves, vulnerable to attack. For example, Amazon's Web Services cloud system was attacked by the Anonymous group over its withdrawal of services to WikiLeaks. Security experts warn that attacks against one user of a cloud provider could take out the service for all others.

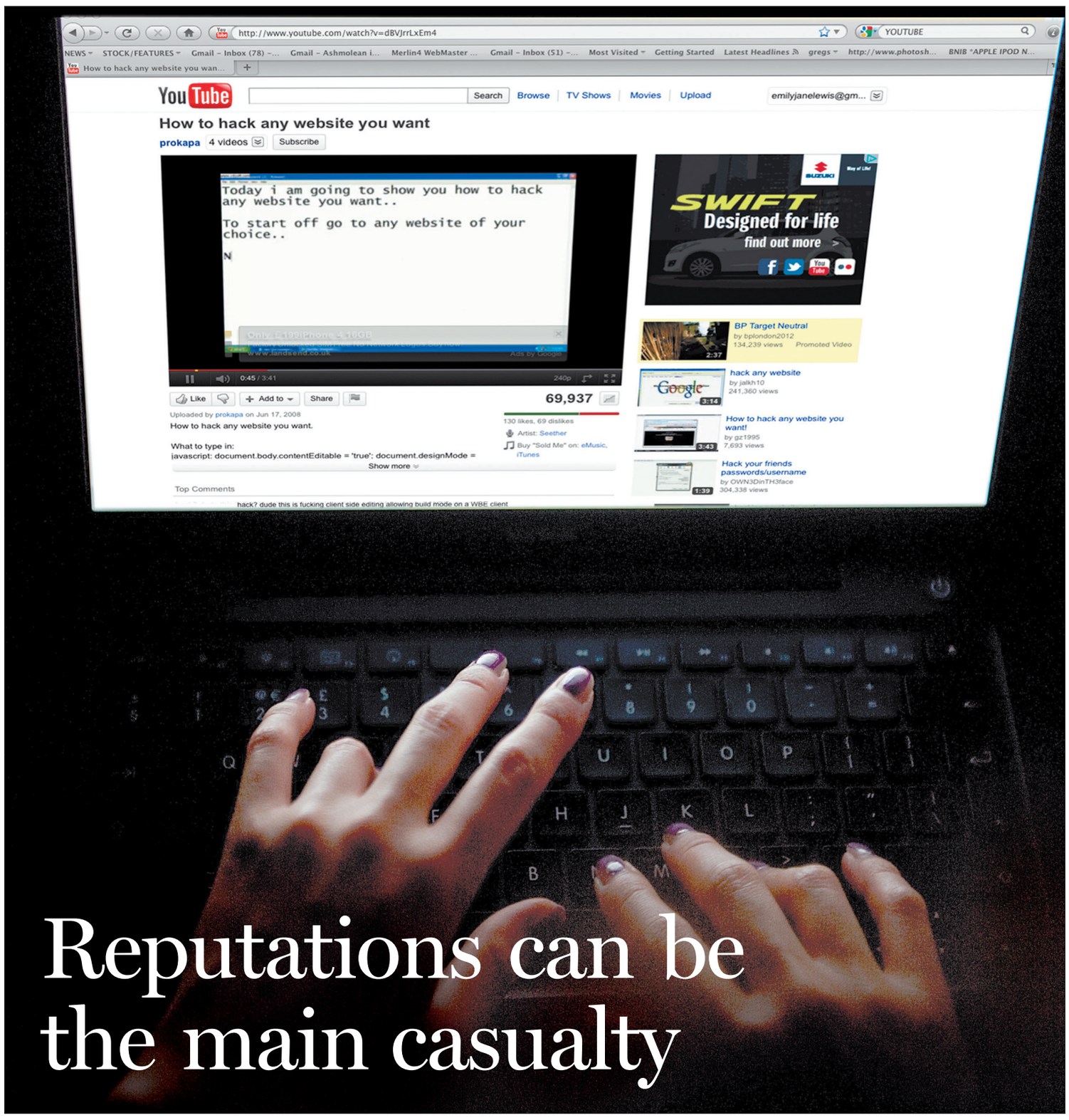
And anywhere that assembles large amounts of sensitive data is likely to prove a magnet for hackers.

"Large providers of cloud services can bring together security expertise and have a really high-powered team defending your data and services, but that also makes a bigger bull's eye for the bad guys to go after," admits Martin Sadler, director of the cloud and security lab at Hewlett-Packard's research arm. "But it's still more of a theoretical than a practical threat."

And, as information becomes more important to businesses, so it will become more attractive to criminals. Cloud providers, in turn, will have to increase their investments in security measures.

"The level of protection in the cloud should be higher [than in the enterprise], because if the service provider is hacked, it is dead," remarks Marc Vael, a board member of ISACA, the security industry body.

"But cloud may become a little more costly," he warns.



Reputations can be the main casualty

Everyday risks

Hackers can find easy lessons online, says **Tim Bradshaw**

Officers at the Boston Police Department were already having a bad day before the phone rang. A thousand usernames and passwords from their union's website had been posted online after a hacking attack, apparently in support of the local instance of the Occupy Wall Street protests.

But when one Bostonian police official answered the phone to a young man with a British accent purporting to be a member of the press, he did not expect that insult would be added to injury.

"We're in the process of investigating it," the official said of the hack.

"Yeah, that was me," the 'reporter' replied.

"You hacked into the website? Would you like to tell me why you did it?" the flabbergasted policeman asked.

"I just got a bit bored," the young man laughed.

Such is the world in which IT security operatives – and, increasingly, public-relations people – now live. This phone conversation was recorded, posted on the video-sharing site YouTube and passed around on Twitter, the micro-communications network, ensuring it received maximum embarrassment for the police and much kudos for the hacker from his peers.

Website defacements and stolen passwords are not a new feature of the online security landscape. But the ease, frequency and profile of such attacks have all risen sharply in the past year, thanks to the antics of Anonymous, Lulzsec and the other hacking collectives that have followed in their wake.

High-profile attacks on the likes of Sony, Nintendo and Rupert Murdoch's Sun newspaper websites have all been executed: for ideological reasons; to make mischief; or, as in the Boston case, simply because the hackers involved had nothing better to do.

"These are people working without a financial motive," says Graham Cluley, senior technology consultant at Sophos, the anti-virus software maker. "Some companies would think that they wouldn't be anybody's target, whereas now people are simply doing it for kicks, or for political reasons."

Imperva, a data security firm, analysed an online forum where tens of thousands of hackers gather to swap tips and brag about successful incursions.

It found that a quarter of the discussions were hacking tutorials, "ensuring", Imperva wrote in its October report, "a steady supply of new talent".

One typical lesson, a four-minute YouTube video, detailed how to hack a website with a relatively straightforward method of hacking a database or web application.

Other popular topics include "denial of service" attacks, whereby a website is overloaded with traffic until it is knocked offline, and spam, unsolicited email containing viruses or links to websites that can capture passwords.

All this is a far cry from the Stuxnet virus, which targeted industrial infrastructure, or the rogue states and organised criminal groups behind sophisticated hacking attacks.

But just as YouTube and blogs have democratised the creation and distribution of media, the social

'It is about raising awareness, because if you do foul up, it is going to be on the front pages'

web has also allowed hacking tools and skills to be shared more cheaply and easily, and the fruits of their application to be seen more widely.

Even if the resulting intrusions do little practical or long-term harm to corporate systems or their users, they are still damaging to an organisation's reputation, especially if not handled and rectified swiftly.

In a recent report, RSA, a security provider owned by storage firm EMC, calls phishing, whereby users are tricked into handing over personal details by a message that appears to come from a familiar or legitimate source, "one of the oldest scams in the book".

Even so, RSA estimates that phishing attacks cost businesses and individuals around the world $520m in the first half of 2011, through tens of thousands of scams mimicking just a few hundred familiar online brands, such as banks.

Phishing attacks are difficult to prevent because they prey on human, rather than technological, vulnerabilities, says Mr Cluley.

He says that weak passwords, using insufficient number or variety of characters, were probably responsible for October's hijacking of YouTube channels of Microsoft and Sesame Street – the latter stunt used to show videos unsuitable for children.

"It's really hard for IT managers to control, because they are putting their trust in users," Mr Cluley says. "Fundamentally, it's about raising awareness and educating users and C-level staff that security matters, because if you do foul up, it's going to be on the front pages."

He recommends repeating the security lessons typically taught at a corporate induction for new employees to long-standing staff every few years too.

The "consumerisation" of corporate IT – as employees bring their own devices such as smartphones and laptops to work and use personal sites such as Facebook – has opened the door to more everyday security risks.

Who goes there? The frequency of attacks inspired by so-called hacking collectives has risen sharply in the past year

Social networks can be venues for phishing, and can also inadvertently give clues to hackers about potential passwords.

CPP Group, which provides credit card insurance and identity protection services, found a third of Facebook profiles contain at least two pieces of personal information, such as a favourite sports team or school, which are commonly used in passwords or security questions.

Consumerisation "is a really huge issue for most of our customers", says Henry Harrison, technical director at Detica, a security firm owned by BAE Systems. "Every IT department is under pressure, particularly from senior executives, to let them bring their iPad to work."

He adds: "Historically, the trend that IT has followed over the past 20 years has been to get tighter and tighter control over computing devices, so the security can be managed.

"Now, people are using a home device with very little control over what other software is on it, and they want to plug that into the corporate network because they find it convenient."

The trick in dealing with such security threats is the same as for more serious technical hacking attacks, Mr Harrison says. "There is a classic trade-off between flexibility and security."

Lawmakers asked to step into digital age

Regulation

Data breaches have brought security centre stage, writes **Alan Rappeport**

US cybersecurity experts say that tough regulations are needed to encourage companies to work harder to protect the data of their customers. However, they fear that government gridlock is allowing the issue to languish.

In the past year, several high-profile security breaches have brought cybersecurity to the fore as an important public issue. This applies to companies as well as to private users.

Citigroup, Sony, Google, Lockheed Martin and Nasdaq OMX have all faced embarrassing attacks that exposed weaknesses in their systems and put sensitive customer data at risk.

Chris Wysopal, founder of Veracode, a cybersecurity company, says that a year ago he surmised it would take several high-profile corporate breaches to spur new legislation – but that now it is unclear what it will take for that to happen.

"I guess it will take a constant drumbeat of these breaches and maybe eventually over time, things will change," Mr Wysopal says. "Or maybe the breaches have to be bigger."

The recent spate of attacks has generated interest in legislation with real teeth, but also pushback from companies fearful of regulatory over-reach.

Last May, the Obama administration outlined a proposal that would give the US government the power to review plans that private owners of infrastructure had in place to defend against malicious hackers.

The White House also called for a US law that would force companies to disclose the loss of customer data to users and federal authorities.

In September, Richard Blumenthal, a Democratic senator from Connecticut, introduced data breach and security legislation that would punish companies for failing to comply with minimum safeguards, require prompt notification of breaches and promote better sharing of technical information.

Mr Blumenthal said: "My goal is to prevent and deter data breaches that put people at risk of identity theft and other serious harm, both by helping protect consumers' data before breaches occur, and by holding entities accountable when consumers' personally identifiable information is compromised."

He continued: "Systems to safeguard such private personal information, and prompt notification in cases of breach, both should be required, along with consumer remedies to compensate for any harm."

Republicans in Congress

'It will take a constant drumbeat of these breaches – maybe eventually things will change'

Chris Wysopal, Founder, Veracode

have called for increased information sharing about security threats between government officials and key industries.

They have also asked for the Department of Homeland Security to obtain more support from the defence department.

The Republican proposal, however, favours companies having broader compliance standards and protection from lawsuits.

In spite of these efforts, political gridlock in the US has dimmed hopes that a law will be created in the near future.

"The US government is so dysfunctional right now that nothing will happen," says Bruce Schneier, a cybersecurity expert. "There's lots of talk, but no real action."

According to Mr Schneier, the US would benefit from a more "cumbersome" approach that challenges companies.

He points to Europe's data protection act and laws in California as models that would be helpful on a national level in the US, but says that companies have been pushing hard for more exemptions to avoid additional costs and negative publicity.

Mr Wysopal says that companies would benefit from national cybersecurity legislation, because it would simplify their problem of navigating the laws that apply in the different US states.

He says that there needs to be a lower threshold for corporate "negligence" when lawsuits are filed against companies for data breaches, so those companies have a stronger business case for investing in security measures.

"Now it's just about brand damage," Mr Wysopal says.

"The whole issue is that people with poor security should have liability."

Meanwhile, the threats are only becoming more challenging, as an evolving ecosystem of devices and software becomes available to new digital users.

The quickly shifting landscape will put added pressure on lawmakers and regulators to act quickly.

According to the Georgia Tech 2012 Emerging Cyber Threats report, mobile browsers, "apps" and cloud computing are presenting new and vulnerable targets for cybercriminals.

Because mobile devices and browsers are infrequently updated or patched, they are rife with security holes.

"Mobile applications are increasingly reliant on the browser," says Patrick Traynor, assistant professor at the Georgia Tech School of Computer Science.

"As a result, we expect more web-based attacks against mobile devices in the coming year."

Cybersecurity

Era of targeted attacks is here to stay

Viruses

A new kind of risk has been found, says **Maija Palmer**

Just in case anyone was starting to feel complacent, researchers have just discovered a new, highly sophisticated virus that appears to be designed to collect information secretly from European and Middle Eastern companies.

Dubbed Duqu the virus is similar to Stuxnet, which was uncovered in 2010 and apparently designed to spy on and disrupt Iran's nuclear programme.

Stuxnet, believed to have been created by a government agency, alarmed IT security professionals because it was so highly targeted and was one of the first times that a piece of malware was able to cause real-world effects in terms of damaging Iranian nuclear reactors.

The discovery of Duqu confirms that the era of cyberthreats is here to stay. Although no one knows quite what Duqu has been created for, it appears to be mining companies for data.

Over the past two years, IT security experts say they have seen more of these kinds of attacks – known as targeted attacks or advanced persistent threats (APTs) – on computer networks.

Hacking attacks in the past used to be widespread and scattergun; for example, sending millions of people an email tricking them into revealing bank details, or hijacking their computer to send out spam messages.

By contrast, an APT is focused on just a few people in an organisation and designed in such a way that it goes unnoticed while it begins a slow and painstaking probe of the network.

Duqu has only been found in some two dozen organisations so far, and security experts are still not sure how it was implanted.

Mikko Hypponen, chief research officer at F-Secure, the IT security company, says: "In advanced persistent threats, an email might be sent to just one company. In will be highly tailored to look authentic, it will be in the right language with the right content, and it tends to go completely unnoticed."

In one case, a director at a UK defence company had a virus on his laptop that had been leaking sensitive details for 18 months before it was discovered.

Defence companies in general came under attack this year in a complex, two-stage operation. First, software was stolen from RSA, the security company, which compromised security tokens that it had issued. A month or two later, defence contractors such as Lockheed Martin, which used these RSA tokens, came under a highly specific assault.

Leaked documents this year also showed that companies including DuPont, Walt Disney, Johnson & Johnson, and General Electric had been hit, as well as law firms and insurance companies. Investment banks such as Morgan Stanley have been attacked and the world's biggest oil and energy companies have been infiltrated.

Henry Harrison, technical director at Detica, a technology consulting company owned by BAE Systems, the UK defence group, says: "People are realising this is something they should be worried about. When we talked about this a year ago, they didn't understand why, but now there has been a change in the level of awareness."

Malcolm Marshall, UK head of information security at KPMG, the professional services firm, says: "Companies have to accept this is inevitable, and begin preparing for how to deal with an attack."

About 50 per cent of the security work KPMG does is with companies that have been subject to such an attack. One of the problems in dealing with APTs is that most appear to come from foreign nation states, such as China and Russia, although the origin of the attack is almost impossible to prove.

When Google revealed its email systems had been the subject of a targeted attack in late 2009, it pointed the finger at China. Privately, security professionals talk about the fact that many attacks happen during the Chinese working day.

It is hard for companies to get redress when the threat comes from these quarters, but practical steps can be taken.

One is to look for unusual network activity. If a developer's laptop begins connecting to an internet address halfway across the world in the middle of the night, for example, it could be a sign of a spy program at work, says Mr Hypponen.

Once rogue activity is detected, it is worth gathering evidence for a while, rather than removing the malware straight away.

Security experts say it is worth trying to find out as much about the attackers as possible, and seeing what they are looking for.

Mr Marshall says: "Having an idea of who is attacking you is helpful for getting a sense of what you need to do to protect yourself, even if being able to prove it in court and litigating is not possible."

Protecting everything in the corporate network is too expensive, but companies can identify their "crown jewels" and put extra security around these parts of the system.

The good news is that targeted attacks can take time to carry out, which means they can be thwarted before critical information has been compromised.

Mr Harrison says: "The traditional view was that when someone got into the network, the company had already lost the battle.

"But in these attacks, the hackers are looking for specific information and it can take them weeks or even months to find it," he says.

"Companies should not despair. It requires thinking about security in a different way, but there are things they can do."

Mahmoud Ahmadinejad, Iran's president, at the Natanz uranium enrichment facility. The plant was the target of the Stuxnet virus in 2010 AP

Banks refuse to pay out to protect clients

Liability

Businesses targeted by criminals are left high and dry by lenders, reports **Joseph Menn**

One of the most lucrative and fastest-growing sectors of the cybercrime economy is the distribution and use of sophisticated software that assists in stealing funds directly from bank accounts.

With most criminals operating from abroad, there is little risk of capture and there are fewer steps than one needs when using stolen credit cards to buy goods that are then resold.

"There has been a noticeable increase in account takeovers that result in fraudulent transfers from the victim's account to an account under the control of the perpetrator," AT Smith, assistant director of the US Secret Service, testified in September to a Congressional hearing on electronic bank fraud, which is estimated in billions of dollars a year. An FBI official said his agency was probing 400 cases of corporate account takeovers with losses of about $85m.

Part of the problem is that the diverse digital underground continues to develop technology quickly. As an example, some members of the pernicious "Zeus" family of credential-stealing programs can intercept authentication codes sent to mobile phones. These illegal business models have also advanced, with effective DIY crimeware kits available free in many places.

But there is a less obvious, and potentially more fixable, reason why the crooks continue to prosper in bank cyber-capers: a standoff over who will pay for better security.

Basically, neither governments nor privately owned utilities, transport and communications companies want to pay to shore up protections against attacks from abroad.

The financial industry has both that simmering argument to resolve and a more immediate one: if a business has its bank account drained by hackers, who should be on the hook, the business or the bank?

In the UK, businesses are often held responsible if they do not recognise fraud on their accounts within two days, says Ross Anderson, professor of security engineering at Cambridge university. Banks sometimes try to shift blame on to individuals, too, he adds.

Under US regulations, the banks generally must reimburse consumers whose accounts are cleaned out. But no such rule protects businesses, even those owned and operated by a single individual.

A small but growing number of companies have been wiped out by Zeus and its ilk, which can be delivered via trick emails that seem to come from a bank or via user visits to legitimate websites that have been infected.

In some instances, US banks have reimbursed companies for all or part of their losses, but they make no promises, and low-level courts have been split so far on whether financial institutions can be held responsible.

The rulings thus far have depended heavily on the exact wording of the contracts between banks and customers who opt for electronic banking, as well as whether the institutions are deemed to have acted in "good faith" with "commercially reasonable" security precautions.

In a big test case, a Maine company called Patco Construction lost hundreds of thousands of dollars after a Zeus infection, then lost money again after unsuccessfully suing its bank.

Institutions are better equipped to catch crooks out Dreamstime

Though the transfers from its accounts were so unusual as to trigger a high risk score from the bank's security service, all that did was trigger "challenge questions". The criminals apparently had the answers because Zeus records keystrokes made on computer keyboards and the same questions had been asked before. The bank won in part because the security rules in effect at the time did not explicitly require tokens, telephone calls or other forms of "out-of-band" authentication.

> Low-level courts have been split so far on whether financial institutions can be held responsible for cases of cybercrime

Another case, heard in Michigan federal court, fell in the other direction. The judge there ruled that the bank Comerica did not show good faith, defined as including "fair dealing", when it did not act quicker to stop wire transfers from client Experi-metal to Moscow, Estonia and China. More than $5m in overdrafts were allowed on one Experi-metal account that typically had a zero balance, the judge wrote after a bench trial.

Doug Johnson, policy analyst at the American Bankers Association, says it is right such cases are decided on specifics. He says revised guidelines published in June will tighten security.

Among other things, the new rules bar reliance on passwords, standard challenge questions and "cookies" that identify specific browsers. He also says a recent survey of 77 banks found that while attempts at fraud had more than doubled in a year, the amounts actually extracted by criminals had fallen.

Though one bill introduced in Congress last year would have extended the protection given to townships and school districts, which have been hit hard by fraud, Mr Johnson says the industry remains opposed to the extension of liability to either non-profit groups or businesses at large.

"Changing the liability model is particularly dangerous for the community bank market," where institutions have less to spend on security and could be ruined by major cyber-robberies, says Mr Johnson. "It is only when you banks and businesses view security as a partnership that it is going to be effective."

But others say that banks are much better equipped than small businesses to outwit crooks.

But if they are not likely to be held liable, they have little reason to spend what it takes.

Mobile devices are likely to be next victims of viruses

Malware

Chris Nuttall looks at recent efforts to keep 'black hats' out

Threats, vulnerabilities, Trojans, phishing sites – the language of PC virus warfare is this year increasingly being applied to mobile devices.

A series of reports from security companies suggest a surge in mobile malware. Juniper Networks says Google Android malware samples grew 400 per cent between June 2010 and January 2011, while Lookout Mobile Security reports a 250 per cent increase in the likelihood of users encountering malware on their mobile devices between January and June this year.

Kevin Mahaffey, chief technology officer and co-founder of Lookout, says 2011 represents the start-up phase for malware "entrepreneurs" developing a business model.

"Every new piece of malware we are seeing is experimenting with methods of distribution – how do you get the malware to people in the first place – and with monetisation – how do you make money as a malware author?" he says.

Distribution is proving easiest in the Android ecosystem.

John Dasher, McAfee senior director of mobile security, says: "Apple has a walled garden, with its curating of apps for its App Store, so it's had far fewer instances of malware, but Android is far more porous."

"There are more than a dozen apps sites, it's very easy to download apps and 'sideload' apps on to a device, and so it's far easier for a hacker to get an app published that contains malware."

The easiest way to infect a smartphone is free games or apps that look similar to well known ones, confusing users into downloading and giving the authors the permissions they need to carry out their underhand tasks.

Malvertising – ads within apps – are also becoming popular. GGTracker poses as a free battery-saver app. Clicking on this takes the user to a fake version of Google's Android Market to download and install the app, which charges premium text messaging fees to that phone.

A more dangerous kind of monetisation spread to Android this year from Symbian, Windows Mobile and BlackBerry smartphones in the shape of Zitmo, a supposed banking authorisation app. It can intercept text messages often sent by banks that provide one-time passwords to help users access accounts and transfer money.

Despite such alarming threats, security experts say the mobile malware problem is minor, compared with the viral warfare raging in the PC world.

"The percentage increases we're seeing are from a tiny base," says Ed Amoroso, AT&T chief security officer.

'How do you get people to adopt a product without selling through fear?' Kevin Mahaffey of Lookout

"Most malware continues to reside on the PC – it's easy pickings there – it's not administered and it's on a big fat broadband pipe."

He says mobile security experts cannot count on learning from their PC counterparts either, with computer security now "in a pretty abysmal state".

With mobile threats still low, mobile security companies are bundling their anti-malware protection with other services to make them more appealing.

"It's a conundrum – how do you get people to adopt a product without selling through fear [that they may face virus attacks]," asks Lookout's Mr Mahaffey.

That is why his company includes useful security utilities such as the ability to locate lost smartphones and remotely lock or wipe them.

The always-on location-aware nature of smartphones makes this possible and their activity on the network means they can easily be monitored for unusual behaviour by mobile operators.

AT&T has 40 researchers working in the field of behavioural analysis to spot malware, rather than relying on the traditional PC-like databases scanned to identify viruses by their software signatures – the fingerprints of their code.

McAfee, acquired by the chipmaker Intel this year, is working on embedding security into the hardware.

"For years, security software has lived above the operating system layer, but the goal is to put security lower in the stack where it can't be tampered with," says Mr Dasher.

Juniper, whose Junos Pulse Mobile Security Suite is used by AT&T and others, advocates a holistic approach of network operators monitoring and blocking threats as well as protection on the smartphone itself.

"There is the need to scan apps as they are being downloaded. Firewalls have to be set up and finally the user has to be educated about threats and safe practices," says Karim Toubba, Juniper vice-president of security and strategy.

3LM, founded by two former members of the Google Android team, last month launched an enterprise security suite for Android that hooks directly into the operating system and gives IT departments a management console to ensure employees' phones are secure.

Tom Moss, chief executive and co-founder, says this is the first of next-generation anti-malware products that should arrive in the next year – just in time.

"Now Google is introducing things such as NFC [mobile payment] chips in addition to other services that have financial components, it just makes Android a bigger target for the 'black hats'," he says.

"Google will take action against them, but there's also going to be a very healthy and robust third-party developer community coming along with security solutions as well."