The Connected Business

Wednesday April 24 2013

www.ft.com/reports | twitter.com/ftreports

Intelligence chiefs warn of increased cyber risks

Paul Taylor discovers security experts on both sides of the Atlantic are calling for closer co-operation with businesses to prevent attacks

Online security has moved to the top of both the political and corporate boardroom agendas in the past year, and there are dire warnings about the consequences of ignoring the threats posed by financially motivated criminals, state-sponsored industrial spies and politically motivated "hacktivists".

Many of the most dramatic warnings have come from current and former US and UK security and intelligence officials, who are concerned about the theft of intellectual property (IP) and the impact of cyber-based industrial espionage on business competitiveness. There are also fears of state-sponsored and other attacks on critical infrastructure, such as utilities, banks and hospitals.

For example, Leon Panetta, then US secretary of defence, warned last year of the danger of a "cyber Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyse and shock the nation and create a profound new sense of vulnerability". (See "Fears of war and espionage raise tensions", Page 2.)

John "Mike" McConnell, a former US intelligence chief, now vice-chairman of Booz Allen Hamilton, echoed the warning, adding the west has had its "9/11 warning" on cyber security and that, unless urgent action is taken, the US faces a "cyber equivalent of the World Trade Center attack" that could bring the country's banking system, power grid and other essential services to their knees.

Asked whether such warnings are justified, Edward Stroz, a former FBI agent who was responsible for the formation of the bureau's computer crime squad in New York and co-founded Stroz Friedberg, a company that advises corporate clients on security issues, says simply: "They are not crying wolf."

Mr McConnell's warning came after a cyber attack on Aramco – the Saudi Arabian oil group – that wiped the hard drives on about 30,000 desktop PCs, a move Saudi and US officials believe was designed to disrupt oil production.

Similarly, a dozen large US banks, such as Wells Fargo, JPMorgan Chase and Bank of America, were last year the victims of sustained distributed denial of service (DDoS) attacks – in which many infected computers target data at one website causing it to crash. These appear to have been orchestrated overseas. The attackers made use of one or more of the estimated 1,500 "botnets" (collections of hijacked PCs) that have been infected by computer viruses or other malicious software. These are available for hire in the cyber underworld.

But while many such attacks appear to be politically motivated, security experts say most are conducted by cyber criminals for monetary gain, or in order to steal intellectual property and trade secrets.

For example, in February the Mandiant Intelligence Center, a US-based cyber security firm, published a report identifying a group linked to the Chinese military as being responsible for "a multiyear, enterprise-scale computer espionage campaign".

Mandiant claimed it was: "One of the most prolific [groups it tracks]

Continued on Page 3

Inside »

On FT.com »

Online threats
Paul Taylor looks at the top 10 dangers
FT.com/video

EU's lawmakers and states take sides over privacy regulations

Data protection laws

James Fontanella Khan on Europe's plans to strengthen individual rights

Brussels' plans to overhaul Europe's outdated data protection laws are set to enter a complicated negotiation phase during the coming months, as lawmakers and member states lock horns over the controversial rules aimed at toughening privacy rules.

Draft rules unveiled last year by the European Commission, the EU's executive arm, which aimed to find a balance between bolstering privacy rights and fostering innovation in the era of the internet, are coming under attack from many sides.

The European Parliament wants to toughen the commission's proposals by imposing stringent rules to protect citizens' privacy – a move that could affect the business model of the growing number of companies that depend on their customers' data.

The European Council, representing EU states, is pushing for a softer approach. It wants to lighten the regulatory burden for business at a time of recession – a move that could leave citizens vulnerable to companies misusing their digital avatars, for example.

What has muddied the waters further is the lobbying effort conducted by the world's largest technological groups, as well as small and medium-sized companies, which have been furiously campaigning to water down the entire legislation.

They fear that the excessive one-size-fits-all regulatory approach could damage the future of business, which is daily becoming ever more data-driven.

Brussels' main objective is to update the EU's current privacy rules, which were agreed in 1995, a pre-Facebook and pre-Google era, when the internet had practically no role in people's everyday life.

Viviane Reding, the EU's justice commissioner, proposed a series of new rules early in 2012 to achieve this.

The overarching goal for Ms Reding's department was to create a single set of coherent rules that would apply across member states. At the moment each country has to guarantee a minimum standard but the degree of application varies substantially from state to state. Everybody likes this as it sets certainty and removes any regulatory bartering.

Companies will have to deal with only one regulator, the one in the country where they have set up their European headquarters.

This move is also welcomed by internet groups that have a presence in multiple countries as they will not have to deal with a plurality of data protection agencies. Given the same rules apply everywhere it is immaterial which watchdog they interact with.

Individuals will now be granted the right to access to their data whenever they want. This is seen as fundamental right for privacy advocates, who are concerned about the enormous amount of information we effectively hand over to private companies.

Businesses, in particular social media companies, take a different view. The "right to be forgotten" – which grants individuals the right to ask an online company such as Google or Facebook to remove any content related to them on the web – is seen less favourably by many businesses. None are concerned about removing items from sites that they have full control over but the challenge becomes more difficult once something goes viral.

> Companies fear an excessive one-size-fits-all approach could damage business

Many member states would scrap this rule but the parliament is adamant it wants to to make it as tough as possible.

Online groups will also have to seek explicit consent from people when using their data for commercial purposes.

This is not a problem in principle but many companies, in particular advertisers, are concerned by the endless amount of times they will have to seek consent from users when using customer data for advertising purposes.

All companies with more than 250 employees that handle data will have to name a data protection officer.

This is fine for large tech groups, which already have privacy officers, but for a mid-sized manufacturer it could become a nightmare. The European parliament is also keen to extend this to small companies but member states fear it could affect small businesses, such as a local butcher or corner shop with a client mailing list.

The other major change is the size of penalties for those companies that breach the regulation. At the moment, national regulators can barely fine companies up to €1m but under the new rules fines would go up to 2 per cent of a group's annual global revenue. For some companies that could be worth close to €1bn.

Ireland, which holds the EU's rotating presidency, is keen to reach an informal agreement on the data protection regulation by the end of the year.

However, many of the EU's 27 members have serious concerns over the draft law, and the parliament made more than 3,000 amendments to the commission's original text. This suggests it will take time and much debate before a compromise is found.

In the end, the commission's plan might represent the true middle ground. Whether this will be also a true middle ground for both privacy advocates and business interests in Europe remains to be seen.

Continental drift: EU commissioner Viviane Reding Getty

Spammer in the works: Mahmoud Ahmadi-Nejad, Iran's president, on a visit to the Natanz uranium enrichment facility in 2008. The US government is believed to have targeted the site with the Stuxnet worm Getty

Fears of war and espionage raise tensions

Global politics Internet sabotage is rivalling jihadist terrorism as the most pressing threat to governments and businesses, writes *James Blitz*

For most of the past decade, western security chiefs have been mainly concerned about the threat from jihadist terrorism and affiliates of al-Qaeda. But top security officials are also having to pay greater attention to the threat of cyber warfare and cyber espionage from foreign state actors and their proxies.

It is the prospect of an epic cyber war that generates most alarm. Leon Panetta, the former US defence secretary, said last year that a "cyber Pearl Harbor" might one day take place.

Experts conjure up the possibility of a cyber war, with enemy states exploding fuel refineries or sabotaging air traffic control systems. Nato even produced an advisory manual on cyber warfare in March, declaring state-sponsored cyber attacks must avoid civilian targets such as hospitals, dams and nuclear power stations.

Yet much of this discussion is speculative and the work being done by defence ministries to build up capabilities remains secret. In contrast, there is a real and present concern about cyber espionage, focusing in particular on allegations China and Russia have state agencies that are "exfiltrating" billions of dollars' worth of intellectual property from western governments and companies.

Both nations deny these allegations. But the issue is fuelling diplomatic friction in relations between Washington and Beijing, with consequences that may not have been fully realised.

The threat of cyber war – the possibility states could launch attacks that destroy infrastructure – should certainly not be ignored. The world witnessed an attempt at industrial destruction via the internet when the Stuxnet worm was launched in the late 2000s, almost certainly by the US and Israel against Iran's nuclear programme. Stuxnet did limited damage to Iran's facilities and the programme recovered. But the incident threw a spotlight on the possibility of major powers inflicting serious damage on infrastructure through the internet.

Meanwhile, the world's leading military powers are secretly putting money and effort into cyber war capabilities. Jarno Limnéll, a director of Stonesoft, a computer security company, says cyber war will be increasingly attractive for three reasons: "It is a predominantly offensive type of engagement that can be hard for a defending nation to contain; it can do the same damage as conventional weapons; and it provides a high level of deniability."

We have not yet had a full-scale cyber war. For now, it is the damage being done by state-sponsored cyber espionage that is worrying western governments and UK and US businesses. Two issues are of concern. First, western states have pointed increasingly to the damage done by such activity, which involves the theft of intellectual property by what are technically called advanced persistent threats (APTs) that infiltrate computer systems.

In the US, a classified National Intelligence Estimate, which represents the consensus view of the US intelligence community, is said to have reported a wide range of sectors have been the focus of hacking over the past five years, including energy, finance, information technology, aerospace and motor manufacturing.

In the UK, BAE Systems Detica, a company that specialises in cyber security, has calculated that UK companies lose £27bn a year through cyber espionage. Sir Jonathan Evans, the former head of MI5, the UK security service, said last year that one UK company had lost £800m of intellectual property in a single attack. British ministers say they know of a UK company that lost 100GB of data in a single incident, roughly equivalent to a 20m page Word document.

Second, there is a growing suspicion the Chinese state plays a huge role in much of this activity. China strongly denies these allegations, and Barack Obama, the US president, mindful his country depends heavily on its economic relationship with China, has been careful not to identify it by name in public.

Still, in recent weeks western officials have started to get more vocal in their criticism. In the US there has been a strong focus in particular on work done by Mandiant, a security firm, which suggests that China's People's Liberation Army has been the main sponsor of an entity carrying out thousands of APT attacks on North American targets. It puts a focus on a PLA unit (number 61398) operating out of Shanghai as it carries out these activities.

China is not the only concern. Russia is privately thought by western security agencies to be stealing information from energy and defence companies. Iran is also becoming increasingly active, not in espionage, but in carrying out highly disruptive "denial of service" attacks on regional states. It is the suspected source of the Shamoon virus that crippled thousands of computers at Saudi Arabia's Aramco and Qatar's RasGas last August.

Still, western states cannot just point the finger at China, Russia and Iran. Some experts say the US and UK are also carrying out such activity. "The truth is that everyone is spying," says Mr Limnéll of Stonesoft.

But this is of little relief to US and UK companies facing the growing Chinese threat. For now, the fundamental task facing governments and businesses is to build up protection against foreign cyber attacks. US lawmakers are preparing to create new punishments for companies from China and elsewhere that use trade secrets stolen by hackers.

In the UK, security services have entered into an information sharing partnership with the top 200 UK businesses, providing them with real-time information when threats appear.

But these are early days. Critics say there is nowhere near enough collaboration between western governments and businesses to face down the threat from foreign state actors – and that the worst of the dangers is yet to come.

On FT.com »

IT & Business
Smart meters signal new era for utilities
FT.com/video

Data breach reports should aid those who have been affected

Compliance

Any leakage of information should be treated as a crime, writes *Rod Newing*

Consumer advocates, politicians and regulators are stepping up the pressure on organisations to report data security breaches – the unintentional release of data that should be kept secure – in a timely fashion, especially when customer information is compromised or privacy is an issue.

It sounds like a relatively simple requirement, but the actual reporting process is extremely complex.

There is no clear definition of what constitutes a security breach, what type or size of breach should be reported, the time limit, who to report to, what to report and so on. Each country has enacted different rules; each state in the US has separate rules; the EU has yet to harmonise and different sectors have their own rules.

"It is a minefield," says Mark Waghorne, a senior manager in the information protection team at KPMG, the consultancy. "Some of them align and some conflict."

He says an international business could be put into an invidious position. If a breach occurs in one country it could be told by local security services to keep it secret, but might be obliged to report in other countries.

Organisations may need to report breaches to those affected, such as employees, customers or suppliers. They may also need to report to banks, stock exchanges, industry bodies and the police. Reporting might be compulsory or voluntary, and the media might need to be informed.

Marc Dautlich, head of information law at Pinsent Masons, a law firm, says the trend for legislation on reporting began 10 years ago in California. "Sharing information was seen as a good way to bring problems to light and to protect customers," he says. "The overriding concern of all regulators is the potential harm to affected individuals. That is why they like you to report incidents, even when not required to do so."

The UK's Information Commissioner's Office says informing people about a breach is not an end in itself. "Notification should have a clear purpose," it says, "whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints."

Not reporting an incident risks regulators thinking the company is trying to hide something. Rob Cotton, chief executive at NCC Group, an information assurance firm, says reporting puts the data owner back in control. "It removes the fear that information will be reported by a whistleblower or appear online," he says.

The best defence is to include reporting policies and procedures in the organisation's security strategy. This may need to set out the "lowest common denominator" of regulations, which could result in some over-reporting.

But it is also important that a focus on reporting does not stop companies acting to reduce the risk of loss in the first place.

Ruggero Contu, research director for security solutions at Gartner, the analyst, says any strategy should include having the tools to report and reveal the effect on data. If data are properly encrypted, a loss may not need to be reported at all, he adds.

Prompt reporting, often within 24 hours, may seem a reasonable demand. But it does not give much time to identify if the incident is genuine, or the nature of the loss and its effects. Reporting internally and bringing in forensic aid can also take time. However, confirming a breach too early could result in revealing unimportant incidents or giving too little detail to satisfy all parties.

Although all communications should be honest and open, it is also important to tell those affected what action they should take. This could involve changing a password, cancelling accounts and opening new ones, for example.

Rik Ferguson, vice-president for security research at Trend Micro, a security solutions provider, says that any internal investigation into a breach should assume it is dealing with a crime scene.

Evidence gathering processes must ensure that anything found could be admissible as evidence, including making sure evidence and facts are not inappropriately communicated externally to preserve their integrity.

"Failing to report breaches makes it difficult for policy makers to understand the overall impact, root causes and possible interdependencies of cyber security incidents," says Simon Bain, chief technology officer of Simplexo, a secure search company. "It also prohibits people understanding and addressing them."

Contributors »

Paul Taylor
Editor, the Connected Business

James Blitz
Defence and diplomatic editor

James Fontanella-Khan
Brussels correspondent

Maija Palmer
Social media correspondent

Jane Bird
Michael Dempsey
Rod Newing
Paul Solman
Jessica Twentyman
FT contributors

Adam Jezard
Commissioning editor

Andy Mears
Picture editor

Steven Bird
Design

For advertising details, contact: **James Aylott**, +44 (0) 20 7873 3392, email: james.aylott@ft.com, or your usual representative

Survival guide Three ways to keep the bad guys out

When it comes to cyber security, it seems the best advice is that only the paranoid survive. So here is a guide to the three most important things you can do to secure your system.

1 Assume you have already been hacked

"Organisations should assume they have been compromised, or that some of the devices connected to your system are compromised," says Amichai Shulman, chief technology officer and co-founder of Imperva, a data security company.

The growth in the number of different types of devices – from staff using personal iPhones to smart meters measuring electricity usage – that may be connected to a corporate IT network has increased exponentially, and these are not necessarily controlled or vetted by the IT department.

Companies are also collaborating and sharing data with more customers and suppliers, leaving their computer networks more open to attack. As a result, security professionals no longer believe you can keep the bad guys out of the system. The truth is most companies have already been hacked. They just might not know it yet.

The latest Data Breach Investigations report from telecommunications company Verizon, published this month, found 66 per cent of all breaches remained undiscovered for several months. Yet the IT security community is not completely defeatist. A security breach is almost inevitable. But there are still plenty of things a company can do to secure data and thwart hackers.

"Saying you are unhackable is foolish, but containing, controlling, and preventing repeat attacks is still possible," says Joerg Weber, head of attack monitoring at Barclays. "We are still in a position to make our opponents' lives very difficult."

Or, as Mr Shulman puts it: "It is not about preventing breaches, it is how fast you react to them. Even if you can respond in a week rather than months, you have done so much better and prevented a lot of damage."

The other good news is many of the attacks and much of the malware are relatively basic.

Mr Weber says: "A lot of people focus on the bleeding-edge computer threats such as Flame [a computer worm discovered last year]. But that was highly targeted and only touched a few thousand people.

"Meanwhile, everyone else is dealing with older, more mundane issues. Boring stuff is still going on. It doesn't have the sexy factor but it is still dangerous," he says.

Computer worms and viruses such as Conficker and Slammer, which were first detected more than five years ago, are still an issue for IT security experts, and one of Mr Weber's daily problems is the Blackhole exploit kit, malicious software that has been around for some time.

According to research by the Center for Strategic and International Studies, a US-based public policy research institution, more than 90 per cent of successful breaches took place using the most basic techniques.

2 Be vigilant

To a large extent, protection comes down to monitoring, monitoring and more monitoring. Leon Ward, field product manager at SourceFire, a security company, says businesses should start with a comprehensive assessment of how their IT system is supposed to behave.

> 'To a large extent, protection comes down to monitoring and more monitoring'

"People do not know what normal looks like, which makes it hard to pick out what is malicious." Here, big data tools can help companies analyse their systems quickly and more thoroughly than before, helping pick up trends they may not have otherwise seen.

Then it is a case of trying to spot anything out of the ordinary quickly. Technology can help perform a "sniff test" on information coming in and out of a system. But, say analysts, nothing beats human eyes.

"The best intrusion detection system is a vigilant systems administrator," says Conrad Constantine, research team engineer at AlienVault. Hackers will always be able to circumvent the "sniffer" technology by creating new programmes, but a good systems administrator will know the computer network intimately, and pick up on even subtle changes.

3 Make IT more employee friendly

Employees remain the biggest weakness of IT systems. The best security protocols are useless if staff simply work around them.

One of the biggest difficulties for security professionals is staff using what is known as "shadow IT" – computer programs that may not have been officially provided by the company but which employees install themselves because they help them do their jobs.

"Often there are whole departments doing stuff outside the governing eye of the company. But you can't protect what you don't know about," Mr Constantine says.

Somewhat counter-intuitively, perhaps, the answer is not to clamp down but to make IT departments more permissive and responsive to staff needs, he says. "Ask yourself why they either weren't aware, or were unsatisfied with, your organisation's own IT service offerings. When IT enables projects instead of acting as a barrier, there is less incentive for people to create dangerous exceptions in governance.

"Think of it as a needle exchange. You are not preventing people from using drugs, but you are saying, if they are going to do it, let's help them do it safely."

Maija Palmer

Biggest danger to intellectual property comes from within

Business link: MI5's London offices. The UK security service is working more closely with companies on IT security issues Alamy

Crime When it comes to stealing data from companies, terrorists and Chinese hackers are way down the list, reports *Michael Dempsey*

One of the common frustrations investigators of cyber crime face is finding a victim of industrial espionage has not maintained a clear audit trail of who has accessed sensitive data.

Especially when, as Jason Straight, New York managing director for cyber investigations at Kroll, says, the primary threat to corporate intellectual property (IP) comes from within.

"You can buy a USB stick that will download a terabyte of data or use file transfer programs like Dropbox to pull down someone else's IP without having to hack into anything. These technologies are very effective for industrial espionage. Malicious insiders now have unprecedented opportunities to steal from a company."

He adds: "We don't see different personal profiles in different parts of the world, we find the insider espionage story playing over and over again."

Businesses need to avert their gaze from high-profile, state-sponsored cyber threats and look at their people. A good employee passed over for promotion can become a vulnerability, for example, or people can be placed in a business just to steal data.

When investigators are called in to find the source of a leak, they often start with an access log detailing who has seen and used information – if that log exists.

Software to keep centralised access logs is easily available, and it gives investigations an immediate starting point. Simple precautions can help. USB ports can be disabled, so only staff needing to use them can do so. Awareness training will let people know why these steps have been taken to reduce a risk of resentment.

The scale of the cyber espionage assault and the alarming technical armoury available to IP thieves can appear daunting.

Some criminals are even using telephone advice lines attached to malicious programs known as malware, which are designed to penetrate networks. They operate by breaching company security and then offering a tour of the victim's internal secrets on a pay-by-the-hour basis.

Cyber security specialist BAE Systems Detica estimates the cost of internet-enabled IP theft from UK businesses at £9.2bn a year with another £7.6bn stolen in industrial espionage aimed at contract bids and other sensitive data.

The group has long worked with intelligence agencies on both sides of the Atlantic and has expanded its commercial activities since a 2008 acquisition by defence company BAE Systems. "It's important not to give up hope," says David Garfield, Detica's managing director for cyber security. "The internet is an enabling technology and you can use it to redress the balance in your favour."

There are some sectors that feel industrial spies will not target them. The defence and aerospace sector is accustomed to the threat, but other parts of the economy have been slow to respond to the dangers.

"Some companies think if they are not in defence, they won't be the target of espionage. But IP theft is pretty systematic and, in a knowledge-based economy like the UK, the removal and copying of IP can have a long-term impact," Mr Garfield says.

> A good employee passed over for promotion can become the weak point in a company's security

Sectors at high risk include pharmaceuticals, biotechnology, IT and chemicals. Mr Garfield's advice is to advance the status of espionage to a risk worthy of board level attention. That task should become easier as the UK government's Cyber Security Information Sharing Partnership (CISP), launched in March, swings into action.

CISP will allow about 200 UK companies to open up over cyber intrusions and work with intelligence agencies and Detica to counter the threat. A Fusion Cell at the heart of CISP involves Detica and will assess sensitive intelligence material to improve information about the threat for partner companies. A revelation last year by the head of the MI5, the UK Security Service, that one national company had lost £800m through IP theft looms large over this initiative.

One former intelligence officer sums up the divide between his world and the private sector by saying: "We [the intelligence community] are indoctrinated in the need for IT security, but that is not necessarily the case for people in industry. For me that's the greater concern."

CISP is meant to bridge that gap. Yet the former intelligence man points out many government initiatives so far have concentrated on financial cyber crime, leaving business unaware that "it's the industrial espionage side of things that's the main target".

He also warns that the recent emphasis on the idea of the defence of critical national infrastructure, such as hospitals and power plants, has also distracted attention. "The only people who'll attack your infrastructure and succeed are other nations, but industrial espionage can be carried out by a whole host of players, and that's a far more important consideration."

As Kroll's Mr Straight says: "Chinese hacking may be the least of your worries."

Intelligence chiefs warn of increased cyber risks

Continued from Page 1

in terms of the sheer quantity of information it has stolen."

China has consistently denied the country's military has been involved in cyber attacks on US corporations and government agencies. Nevertheless, the US administration, which has until recently avoided direct accusations against its economic rival, appears to have adopted a tougher public stance on the issue.

Just last month Tom Donilon, the White House national security adviser, spoke of the "targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale". It was the first public denouncement of Beijing by a senior US official on this subject.

More generally, the past 18 months have seen a further dramatic increase in the scale and financial damage caused by cyber attacks. As the 2012 Data Breach Investigations Report, published by Verizon Communications, notes: "Perhaps more so than any other year, the large scale and diverse nature of data breaches and other network attacks took centre stage."

Verizon's latest report is based on analysis of more than 47,000 reported security incidents and 621 confirmed data breaches in the past year. The report says 37 per cent of breaches affected financial organisations, and notes "a definite relationship exists between industry and attack motive, which is most likely a byproduct of the data targeted". So, for example, retailers would be targeted by groups looking to steal credit card details and manufactures would be the victims of industrial spies seeking IP information.

The report supports the contention that, not only have the threats facing companies increased in number, they have also grown in sophistication to include both advanced persistent threats – groups that have the ability to make frequent and repeated attempts to break into systems and launch DDoS attacks.

While it is difficult to measure the full effect of cyber attacks, Symantec, the security software company, estimated the global cost of cyber attacks in 2011 was $338bn in financial losses and remediation.

> 'Along with technology comes the risk attackers will try to disrupt our way of life'

What is clear is that cyber criminals, including state-sponsored elements, now have access to enormous resources. "Early last year, a different type of DDoS attacker emerged: one with considerable botnet resources, but also an intimate understanding of how the internet routing topology works," says Prolexic Technologies, which specialises in DDoS protection services.

"When you have average – not peak – rates in excess of 45 gigabits per second and 30m packets-per-second, even the largest enterprises . . . are going to face significant challenges," says Stuart Scholly, Prolexic's president.

The proliferation of employee-owned mobile devices in the workplace, coupled with much more porous networks designed to accommodate remote workers, supply chain partners and customers, means old security models such as corporate firewalls no longer work.

Experts instead suggest that, in addition to investing in the latest generation of cyber security tools, including those that are designed to spot unusual or unexpected behaviour, companies need to identify their most valuable digital assets and focus on protecting them.

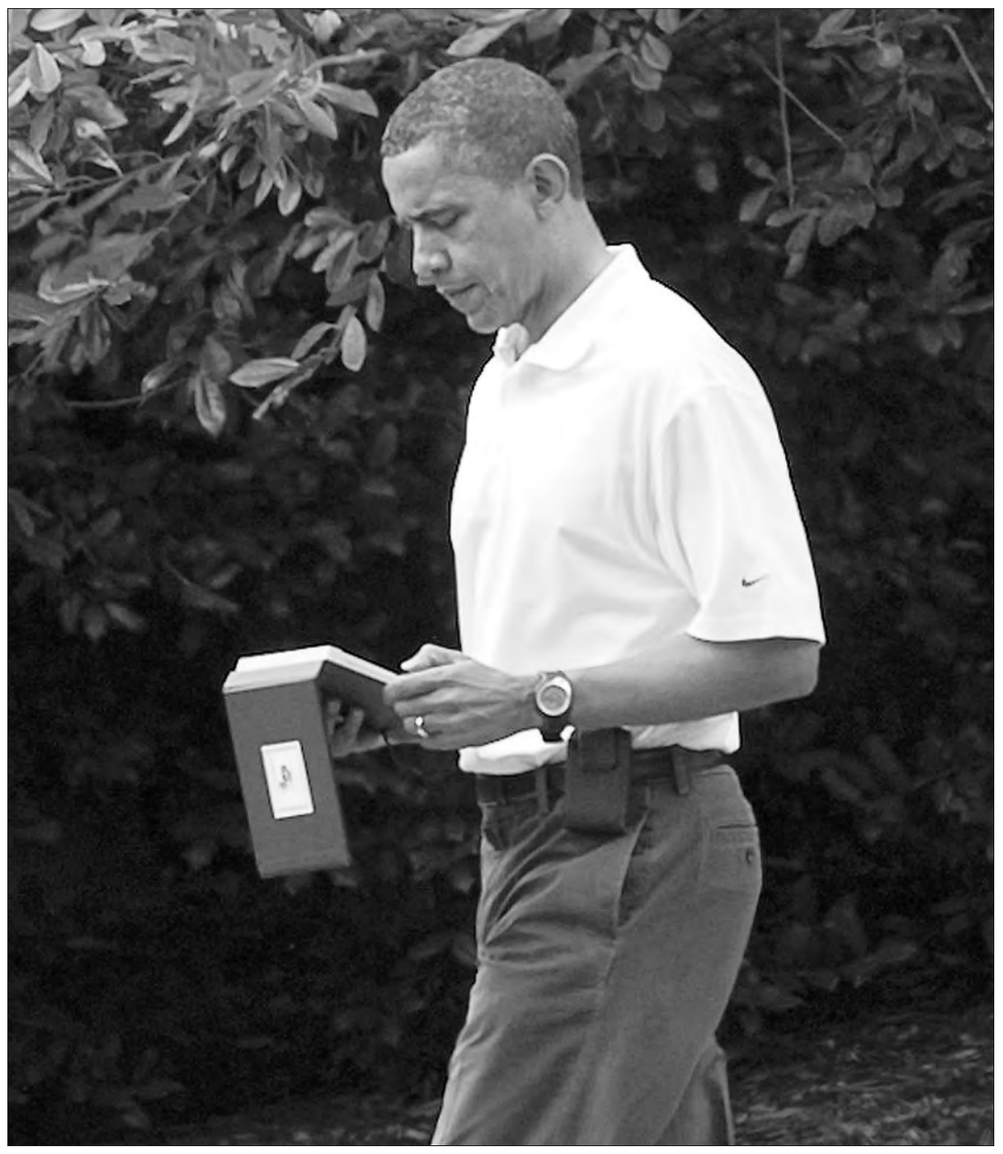
David Burg, a partner at PwC, says: "It is extremely important for company chief information security officers today to foresee threats, protect data and intellectual property, respond efficiently to crisis, and offer strategies and solutions for staying secure in an increasingly dangerous environment."

Hugh Thompson, chief security strategist for technology company Blue Coat Systems, says: "We're at a pivotal time in information security. Technology has transformed the way we shop, the way we bank, the way we socialise, the way we run an enterprise and the way we live.

"Along with the powerful transformation that technology has fuelled, there comes the risk that attackers will try and leverage technology to disrupt our way of life.

"The rash of highly targeted attacks over the past two years is testament to the fact the adversaries we face are sophisticated and determined."

Vigilance over supply chains will reduce contamination



All the president's data: Barack Obama has warned of cyber security threats
Getty

Minimising risk Constant monitoring is the best form of protection, reports *Jane Bird*

It seems that even shrink-wrapped products on retailers' shelves may not be free from the risk of infection by malign forces. As Europe's horsemeat in beef burgers scandal has shown, the complexity of supply chains can make it almost impossible to guarantee the integrity of a product assembled from many remote sources.

According to Amrit Williams, chief technology officer of California-based Lancope, a network security company, Russian criminals have hired scientists to create pirate copies of Microsoft's Windows. "They seem innocuous because they are shrink-wrapped and [hologram protected]. But once loaded in corporate environments, they can easily bypass security controls."

Microsoft has long warned about counterfeit software, which it says "lurks around every corner and can find its way into business settings".

Counterfeiters spend a lot of time, it says, making illicit software-purchasing sites look like the real thing.

An investigation Microsoft conducted into pirate software in China found 91 per cent of fake products contained malware – programs designed to do harm – or deliberate security vulnerabilities.

Concerns that malware that could be used to damage or steal data might be incorporated into computer hardware or software before leaving the factory were highlighted in a report from the Intelligence Committee of the US House of Representatives last year.

This followed a year-long investigation into two of China's biggest telecoms companies, Huawei and ZTE.

The report was scant on hard evidence, and the companies denied the allegations.

However, in a television interview last month, Barack Obama, the US president, said the country had seen "a steady ramping up of cyber security threats. Some are state-sponsored. Some are just sponsored by criminals."

But the creation of a "back door" for hackers in the supply chain may not be deliberate. Last year, some Samsung Galaxy S III smartphones were sold with an accidental vulnerability that could have been exploited by criminal gangs.

To tackle deliberate hacking attempts, companies need to check that suppliers meet rigorous security standards, says Garry Sidaway, global director of security strategy at Integralis, a subsidiary of NTT Communications.

This means having legal agreements that document your requirements with suppliers and checking regularly to ensure compliance is adhered to.

However, to check each supplier can take a week and the costs will mount up. Additionally, many supply chains are now so long that it is almost impossible to know who all your suppliers are.

Steve Keifer, vice-president of global marketing at GXS, a cloud-based integration company, says the introduction of electronic "pedigrees" is starting to improve traceability.

GXS is developing a commercial supply chain risk management tool. This will help companies identify suppliers by showing how they are interconnected, rather like finding contacts on LinkedIn or friends on Facebook.

Another good measure is to implement the principle of "least privilege". This means you grant access to your data only to those who need it and regularly review who is authorised to view it.

Using updated firewalls to restrict the applications outsiders can use also helps – rather like giving them keys that only open specific rooms in a building.

Without restrictions individuals can roam free, says Brian Laing, vice-president at AhnLab, a US antivirus specialist. It is as if you had left a tunnel into your business unguarded.

He recommends isolating servers used for crucial data, such as product development, and using servers for distribution of information that are monitored and have limited access.

"Hackers are looking for the weakest link, even if it's just one server letting them in," Mr Laing says.

Many businesses inadvertently expose information about their supply chain, says David Gibson, vice-president of strategy at Varonis, a data storage specialist.

A survey by his company of 200 organisations found 30 per cent were confident information they held about suppliers and customers was protected.

Some 27 per cent of respondents did not know who was using the information in their organisations; only 22 per cent knew who was responsible for it; and just 37 per cent regularly reviewed access rights.

Companies should assume goods further up the supply chain have already been compromised, says Lancope's Mr Williams. This means constantly looking for anomalous or illicit behaviour.

"For example, you need to know whether your computers should be communicating with hosts in Ukraine or Taiwan and, if not, recognise this as evidence of malicious activity."

Personal device use is challenge for IT bosses

Consumerisation

Training and policies will boost security, says *Paul Taylor*

Corporate IT departments once frowned on the use of personal devices at work, though they often turned a blind eye to "shadow IT" – personal WiFi hotspots, external hard drives and other paraphernalia set up inside corporate firewalls by frustrated but technology-savvy workers.

Many IT professionals also looked askance at the proliferation of laptops, smartphones, tablets and other consumer devices that have found their way into offices as part of a trend known as "consumerisation" and BYOD (bring your own device).

IT departments used to view such devices – particularly those linked to corporate networks, with or without company approval – as a security threat and a support nightmare.

According to a study by Ovum, a UK-based market research firm, commissioned by the data services company Logicalis UK, 57 per cent of employees take personal devices to work.

Significantly, 18 per cent of respondents said their employer's IT departments do not know they are using personal devices, while 28 per cent said their IT departments ignore it.

But times and attitudes, have changed. Many IT departments realised that instead of blocking a trend often backed by senior managers because of the flexibility and productivity associated with it, they may as well embrace and assist it, while seeking to improve security.

Security experts say such measures are essential because of a shift in the corporate security model. "There has been a generational change," says David Murphy, chief operating officer of Blue Coat Systems, a web security specialist. As access to their corporate IT systems has expanded to include customers, partners and suppliers, it is no longer sufficient to secure the corporate perimeters, he says.

The scale of the challenge, particularly related to mobile devices, is daunting. IDC, the IT research firm, estimates more than 1.19bn workers – 34.9 per cent of the global workforce – will use personal technology this year.

Businesses of all types and sizes are considering how best to protect sensitive data and bolster privacy. In some cases this means working with manufacturers, service providers and third-party software vendors to devise a strategy for securing mobile devices.

Samsung has introduced schemes to help companies choose devices that meet security needs, while allowing employees to use both personal and corporate data securely and safely.

Similarly, third-party mobile device management software from Good Technology and others allows IT departments to securely and remotely manage mobiles, while the latest version of BlackBerry's enterprise server, BES 10, lets users of BB10 smartphones – such as the Z10 – toggle between secure personal and work modes.

Vincent Geake, director of secure mobility at BAE Systems Detica, says: "In the days of the PC, the enterprise was able to mitigate [risks] by implementing industry-standard security across each desktop computer, providing a known level of protection using proven products. Now employees work on a range of personal devices, so a company must assess the risk from devices that hold important information, and consider whether they have invested in the necessary security measures to protect that information; these measures should include a combination of technology, usage policies and training."

Significantly, a growing number of industry associations are rising to this challenge in an effort to help members. For example, BITS, the technology policy division of US-based Financial Services Roundtable, has published a paper called Security for Bring Your Own (Mobile) Device, outlining best practices for financial institutions wanting to allow employees to use their their devices to access corporate resources.

"As employees increasingly push to use their own mobile devices in the workplace, it is critical for institutions to clearly define their BYOD policy," says Dan Madsen, vice-president at US Bancorp, a financial services company.

'Tablets left on a train pose less of a threat, as they can be locked and wiped remotely'

"A well-designed policy and effective policy management will allow institutions to take advantage of emerging mobile technologies," he says.

Others, including Google, whose Android operating system now powers the majority of smartphones, argue that while consumerisation and mobility can make it more difficult to secure a business, they constitute less of a security concern for organisations working in the cloud.

"Using a cloud-based service such as Google Apps for Business to store and share information means that important information is accessed through devices but is stored in the cloud," says Marc Crandall, head of global compliance for Google Enterprise.

"This way, the risk of losing company data on a lost or stolen device is significantly reduced," he adds. "If organisations are working in a BYOD environment, we encourage them to put strong internal security policies in place.

"With proper policies, even tablets or laptops left on a train or in the back of a taxi pose less of a threat, as they can be locked and wiped remotely."

Crooks turn to 'spear-phishing' to reel in targets

Persistent threats

There are definite times when alarm bells should ring, says *Paul Solman*

In the early days of the world wide web, sustained and frequent attacks by outsiders against corporate networks often took the form of viruses and malware – software that is designed to cause harm.

A computer user might open an email and unwittingly launch a program that would spread through the machine or network, deleting files or rewriting code. Such threats remain, but as the internet has evolved so have hackers' tactics, and organisations face increasingly sophisticated attacks.

One problem is the spread of social media. The price of the revolution in business and personal communication has been that new avenues have opened that allow cybercriminals to penetrate networks.

"The social media threat has become very prevalent," says Simon McCalla, chief technology officer of Nominet, the UK internet registry.

Sites such as Facebook and LinkedIn often provide cyber criminals with the kind of personal information that allow them to target employees directly.

"We have seen quite a lot of high-profile attacks on big businesses, where the perpetrators were able to log into systems and make changes without having to write a single line of code," says Mr McCalla.

This so-called "spear phishing" is the cyber criminal's favoured means of infiltrating networks, according to research by TrendMicro, the IT security group. Personal details, often gleaned from social networks, are used to tailor phishing emails to a person's interests and convince them to take the bait.

Mr McCalla says: "We've all seen those phishing emails that come from banks asking for our account details. Usually, they are quite easy to spot, especially if they're from a bank you don't even have an account with. But spear phishing is a much more targeted attack and can be very effective.

"If somebody called at your front door trying to sell you a fake watch, you would send them away immediately, but we let our guard down a bit when we go online because it's not an environment that we've been used to and trained up to spot fraudulent activities in."

Another increasingly widespread threat comes from the trend of "bring your own device", or BYOD, where employees use their own devices such as smartphones and tablets to access their employer's network.

Ninety-three per cent of employees admit to violating policies designed to prevent breaches and non-compliance, according to a recent report by the CEB, the US-based business advisory group.

"BYOD opens up an additional channel for the criminal," says Robert Siciliano, US-based online security expert for McAfee, the IT security group. "BYOD devices don't have the same security as the enterprise's networks.

'Ninety-three per cent of employees admit to violating policies designed to prevent breaches'

"Whatever data are contained on them can become accessible. They can become infected with viruses, and these can spread to the network."

Not that the threat from malware and viruses – programs designed to harm or subjugate computers to a hacker's control – has gone away. Indeed, hackers' techniques have become increasingly innovative.

"The technical threat is still large-scale," says Mr McCalla. "Denial of service attacks, the 'hacktivist' attacks that we've seen in recent years, which tend to be co-ordinated and organised by groups. Clearly that threat is still significant. And it is challenging to protect yourself against – even big companies struggle."

Malware attacks have become so successful at penetrating defences that, on average, malware events occur at a single organisation once every three minutes, according to FireEye, a network security provider.

"If you receive something that looks unusual, or from someone you don't know, or if it's too good to be true, or asks you to change your password, that should ring the alarm bells," says Mr McCalla.

"Malware and viruses are essentially an arms race," he adds. "You can mitigate the risk a lot by just making sure your systems and patches are up to date. A lot of these hacks exploit weaknesses where users haven't chosen to upgrade or install the latest patches. Older versions of software are more vulnerable."

This is a point echoed by Mr Siciliano, who emphasises that employees should make sure their home networks and personal devices use security procedures – virus protection, firewalls, password protection – that are comparable with those at their workplaces, especially if they are using them to access work-related information. He advises extra caution when using public WiFi connections.

"Devices such as smartphones, tablets and computers should be shells so that data are held not on the device but on company networks or in the cloud," he adds. "If the device is stolen then no data will be lost."

Increase in danger level has forced security leaders to evolve

Management

The problems for chiefs can change daily, writes *Jessica Twentyman*

Information security has always been a high-stakes game but for the person charged with safeguarding an organisation's data it is one that is daily becoming harder to win.

Recent cyber attacks on banks in the US, the Netherlands and South Korea have put the entire financial services industry on alert. At the same time, they demonstrated to chief information security officers just how difficult it has become to anticipate the rules of engagement their opponents will use.

These cases involved denial-of-service attacks, fuelled by political motives, which took online services offline for hours. However, the issues that the average financial services data security leader faces daily are more wide-ranging, according to David Cripps, chief information security officer at specialist bank Investec.

He says: "It's a constant battle to understand the types of attack we're seeing, keep one step ahead of the attackers, and communicate the risks we face to employees and customers without bombarding them with information."

He says he and his team scan a constantly changing regulatory landscape, in which rules have become far more stringent and more rigorously enforced in recent years, to ensure the organisation is securing its data in a way that will satisfy banking authorities.

Across all industry sectors, about 42 per cent of organisations now employ a specialist who has ultimate responsibility for information security, according to management consultancy PwC. In financial services that proportion is likely to be significantly higher.

But the information security leader role is changing. A report from US-based Wisegate, an online community for IT professionals, says the role has evolved from "a glorified IT security administrator, babysitting firewalls and cleaning malware from infected systems, to holistic risk management, firefighting security breaches and anticipating fires before they start".

Holding down the role today is less about patching up systems and analysing network traffic and more about being able to understand, influence and implement business risk decisions, from privacy policies to disaster recovery plans.

In its annual Global Information Security Workforce Survey, ISC2, an industry membership organisation, found communication skills are now a more critical success factor for post holders than technical knowledge, although "a broad understanding of the security field" still tops the list of desirable attributes.

The evolution from a technical to a strategic role is reflected in the course Mr Cripps' career has taken. He has a degree in electronics, and started as a network manager, but more recently he completed a master's degree in internet and telecommunications law. "Having that kind of understanding of international legislation has been essential to me in terms of being able to fulfil the role as it is today."

This is a view echoed by Stephen Bonner, now a partner at management consultancy firm KPMG, but previously global head of information risk management at Barclays. "I started out in very technical roles, but over the course of my career, I've had to get to grips with things like records management and data privacy."

A rapidly evolving threat landscape, he adds, means education and professional development continues at a frantic pace for most post holders.

Mr Bonner says: "The change I see coming now is very much in line with what we've seen over recent weeks: the rise of so-called 'hacktivists' launching denial-of-service attacks to push political views, or nation states trying to gain economic advantage by stealing information. Broadly speaking, organisations that are compliant with even the most strenuous regulation are still vulnerable to those things, so that's driving a real change in the chief information security officer's role."

Stephen Bonner: the sky is not always falling

Post holders also need to be level-headed, credible influencers in their organisations, translating perceived risks into reasonable defence strategies.

Those that do well, says Mr Bonner, are "those that can convince others from outside the specialism of the validity of their concerns, without constantly claiming the sky is falling, the outlook is terrible and no investment is ever going to be enough to counteract the risks".

But the denial-of-service attacks launched against banks since the start of 2013 show that there is no room for complacency. As PwC's security survey says: "Today's information security leaders . . . know that the very survival of the business demands that they understand security threats, prepare for them and respond to them quickly."