FT SPECIAL REPORT

Cyber Security

Friday June 6 2014

www.ft.com/reports | @ftreports

High-profile hacking provokes public fears

Attacks online have made internet crime a widespread concern but knowledge of how to fight back is lacking, writes *Hannah Kuchler*

The dark world of cyber crime is slowly being prised open, as threats rise to levels where companies and individuals are forced to treat the matter as of critical importance.

Large scale attacks on retailers including international online marketplace eBay and Target, the US chain, have made everyone from executives to shoppers more aware of the threat hackers pose to the online world.

Long spoken of in hushed tones, cyber warfare now finds itself plastered on FBI "Wanted" posters. The US in May brought criminal charges against five of China's military officers for cyber crime.

Law enforcement authorities are grappling with a complex online threat that knows no national borders. In some simpler cases, they have found real-life doors to break down to arrest cyber criminals.

Lee Weiner, senior vice-president of products and engineering at Rapid 7, IT security data specialists in Boston, Massachusetts, says companies are increasing their investment in cyber security in the face of "outstanding" economics for cyber criminals, the majority of whom are motivated by the money they can make.

"The awareness of cyber crime has definitely increased because of the severity and frequency of attacks," he says. "It is more of a boardroom topic now, which hopefully will let companies allocate greater budgets to it."

Illustration: Øivind Hovland

The number of companies reporting concerns about cyber security to US regulators more than doubled in the past two years to 1,174, according to official data. Commercial bankers and oil and gas producers were among those most worried about attacks.

The theft of millions of items of customer data – including credit card details and passwords – is a relatively easy issue to understand compared with the complex world of cyber espionage, nation state actors and illicit markets in intellectual property.

The Target and eBay attacks reverberated through boardrooms across the world. Directors watched closely as Target's chief executive resigned, with under-investment in security seen as partly to blame.

Cyber attacks have wreaked damage on companies for years, but their cost has often been hard to calculate. In the Target case, customers took flight and earnings suffered. "Target definitely helped with the wake up call because of the timing, the magnitude and the subsequent impact to the business, including the chief executive," says Mr Weiner.

'Awareness of cyber crime has definitely increased due to the severity of attacks'

The impact of the hack on eBay, announced in May, is not clear. A cyber criminal penetrated eBay's network using employee credentials and stole encrypted passwords and personal details such as addresses and birth dates. Some cyber security experts question how a hacker was able to access the full customer database. Others suggest that eBay – perhaps surprisingly for a company that owns online payment system PayPal – did not have the most advanced encryption levels.

Continued on Page 3

Kremlin alleged to be waging online campaign against Kiev

Military

Western analysts sense unequal 'war in the shadows', writes *Sam Jones*

Access blocked: Kiev may have struggled to know even the level of threat it faced Reuters

Russia's physical invasion of Crimea may have begun in late February, in the days after the removal of Ukraine's president Viktor Yanukovich, but the infiltration of Kiev's computer systems began years before.

While only glimpses have yet emerged as to what the scope of hostilities in cyber space might be, most military analysts are in little doubt that the Ukraine crisis marks a key point in the so far limited history of cyber warfare.

As far as the intelligence services of the larger Nato-states are concerned – and many private sector security and cyber experts agree with them – the Kremlin is engaged in waging a sophisticated cyber campaign that the authorities in Kiev have struggled to even know about, let alone combat.

"A war in the shadows is in progress in a very active way," says Jarno Limnell director of cyber security at Intel, who holds a doctorate in military science.

"Lots of things have been happening in Ukraine. In the future there will be a cyber element to every war. It's already hard to imagine a conflict without a digital front to it. And that is certainly the case in Ukraine."

Mr Limnell warns against misusing terms: "We should be very careful when we talk about cyber war," he says. "Cyber activities have not produced a revolution in military affairs but an evolution."

A remarkable thing about the cyber dimension to the Ukrainian conflict has been its lack of visibility. Some assumed early on that no cyber attacks were occurring. In the early days of Russia's incursions, the communications of Ukrainian armed forces on the peninsula were not interrupted by far-flung hackers in Moscow basements but by soldiers with boltcutters.

Across the rest of Ukraine there were website defacements or attacks crippling access to service. The kind of acts of digital vandalism assumed to be the first-use weapons in the cyber arsenal, these were low-key or of limited duration.

Groups such as the pro-Russian "cyber Berkut" have had minimal impact.

Cyber Berkut attacked Nato's websites in March with a large-scale "distributed denial of service", or DDoS, assault (whereby multiple false requests for information by a network of hijacked computers overwhelms a website, making normal usage impossible).

'It's unlikely to be hacktivists. The sophistication level is too high and extremely stealthy'

Arbor Networks, which monitors DDoS attacks worldwide, has observed little activity directed against Ukrainian computer systems in recent months. The few such attacks on Ukraine are dwarfed by those seen elsewhere in the world, according to the company's digital attack map.

When Russia invaded Georgia in 2008, the latter saw almost all of its internet services knocked out by denial of service attacks. Although unlinked to any recognised military action, in 2007, Estonia saw government, bank, and media websites over-run after the relocation of a Soviet-era war memorial, the Bronze Soldier of Tallinn.

Since 2010, BAE Applied Intelligence, the cyber security arm of the UK defence contractor, has monitored a virulent piece of malicious software – "malware" – in Ukrainian systems. BAE analysts dubbed it "Snake", though it also goes by the names Ouroburos – the tail devouring serpent of Greek myth – and Sengoku – a Japanese word describing a time of civil strife.

Of the 56 samples of Snake malware BAE analysts were handed over the past four years, 32 came from Ukraine. Of those, 22 were reported in the past two years. BAE believes that dozens, if not hundreds, more systems will be infected

"There are all sorts of digital footprints left by the attackers" says Dave Garfield, managing director for cyber security at BAE. "It's unlikely to be hacktivists who made this. The level of sophistication is too high. It is very well written – and extremely stealthy."

Many markers point to Russia as the malware source – time stamps left in the code and Russian names, for example. Some observers express scepticism about using these to apportion blame, but western intelligence experts are quick to corroborate what the markers indicate.

Snake's capabilities are widespread but fundamentally it is a highly sophisticated espionage tool. After it has infected a computer, it buries itself deep within the existing system, concealing itself from all but the most sophisticated scanning systems. It can exfiltrate whatever information its operators desire, from personal emails to military plans.

Military sources say there is little doubt that Russia is using such malware to obtain up-to-the-minute operational intelligence about what is going on in Ukraine and that it is using it effectively.

"Clearly, cyber was a huge part of what Russia has done," General Philip Breedlove, Nato supreme allied commander Europe said in a public speech in Canada on May 6.

Snake, perhaps more worryingly, is a pathway for its operators to escalate events rapidly if they choose. According to BAE's analysis, the malware is a "digital beachhead", allowing its operators to deliver whatever other malicious code they wish to the heart of infected systems.

"Russia not only now has complete informational dominance in Ukraine", says one intelligence analyst, "it also has effective control of the country's digital systems, too. It has set the stage"

All of which perhaps underscores the point that in cyber space, just as in the real world, tactics follow an age-old playbook.

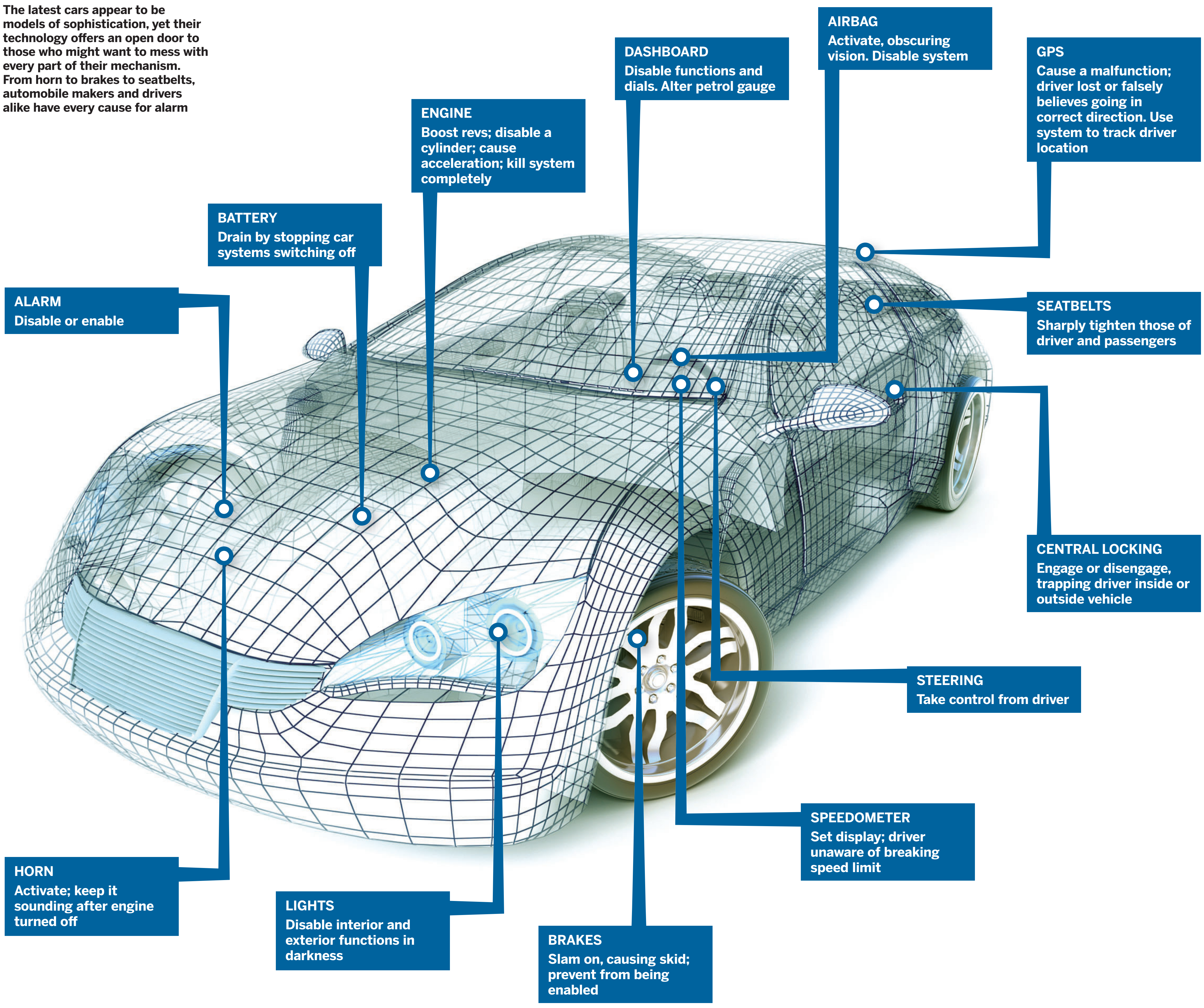
WHEN YOU ARE PASSIONATE ABOUT SOMETHING,
YOU PROTECT IT IN THE BEST WAY.
ZURICH INSURANCE.
FOR THOSE WHO TRULY LOVE THEIR BUSINESS.
ZURICH®

Nice set of wheels, but who is doing the steering?

Automotive industry Despite manufacturers' bravado, car buyers may find themselves with less control than they think, writes *Henry Foy*

What cyber attackers can do to your car

The latest cars appear to be models of sophistication, yet their technology offers an open door to those who might want to mess with every part of their mechanism. From horn to brakes to seatbelts, automobile makers and drivers alike have every cause for alarm


ALARM
Disable or enable
BATTERY
Drain by stopping car systems switching off
ENGINE
Boost revs; disable a cylinder; cause acceleration; kill system completely
DASHBOARD
Disable functions and dials. Alter petrol gauge
AIRBAG
Activate, obscuring vision. Disable system
GPS
Cause a malfunction; driver lost or falsely believes going in correct direction. Use system to track driver location
SEATBELTS
Sharply tighten those of driver and passengers
CENTRAL LOCKING
Engage or disengage, trapping driver inside or outside vehicle
STEERING
Take control from driver
SPEEDOMETER
Set display; driver unaware of breaking speed limit
BRAKES
Slam on, causing skid; prevent from being enabled
LIGHTS
Disable interior and exterior functions in darkness
HORN
Activate; keep it sounding after engine turned off

Source: FT research

Image: Dreamstime FT graphic

You are travelling at 70 miles an hour down the motorway. Suddenly, your dashboard goes blank. The horn starts sounding. You push on the brakes but they fail to work. Then the steering-wheel starts to turn by itself.

Your car is not breaking down. It has been hacked.

The terrifying prospect of a uncontrollable vehicle is becoming a palpable danger, as the rapid advancement of technology means more parts of cars are controlled by computers that can be accessed and exploited by potential hackers.

Self-parking systems are designed to make parking easier, but could be used to take control of the car's steering. Remote key systems should make a car harder to steal, but can also be used to lock a driver inside. And electronically-controlled brakes are meant to make cars safer, but could do the opposite.

"Hacking a car is not that difficult. They are getting increasingly networked," says Fionnbharr Davies, technical director at Exploitable Labs, a company that helps businesses assess security weaknesses. "Essentially, the more complexity you add into a system, the more vulnerable it becomes," he adds.

"The more that is going on, the more that can go wrong."

Software experts, academics and professional hackers have shown that with physical access to a car, such as in a mechanic's garage or a service station, or through MP3 sound files on a CD containing malicious software, data can be uploaded that grants access to outside controllers.

Given that new cars boast a plethora of "connected" applications, from email readers to music streaming services and Bluetooth connectivity, remote access without any physical contact with the car could soon be possible. Some say it already is.

Charlie Miller and Chris Valasek wrote in a paper last year: "Drivers and passengers are strictly at the mercy of the code running in their automobiles and, unlike when their web browser crashes or is compromised, the threat to their physical wellbeing is real." The cyber security experts describe how they took control of a Ford Escape and a Toyota Prius using software code.

In their study, Mr Miller, who works as a computer security expert for Twitter, and Mr Valasek, the director of security intelligence at IOActive, disabled the brakes and other functions of the cars in a series of tests.

This was supported by a grant from the Defense Advanced Research Projects Agency, part of the US defence department.

The pair took advantage of small electronic control units that are built into virtually every new car and control almost all the vehicle's systems, from central locking to fuel injection, window opening and climate control.

"The software that is running on [cars] probably has not been thoroughly audited. It's very fresh," said Mr Davies. "They have been in their little bubble for quite a while and now they are being exposed to the internet and all that."

Ford said that while the vehicle was hacked by Mr Miller and Mr Valasek, it required both direct access to the vehicle and the ignition key.

"This extraordinary effort, with direct physical connection to the vehicle, was neither remote nor wireless and does not suggest that Ford vehicles are generally vulnerable to cyber attack," says Christin Baker, a Ford representative.

"We continuously work to ensure that all our electronic systems have robust security protocols."

Toyota says it has developed effective firewall technology to prevent remote access to its vehicles, and that "we continue to try to hack our [own] systems".

But behind closed doors, the car industry is concerned about this new reality and whether it has the ability to stay ahead of potential attack methods, according to numerous officials at carmakers who spoke to the FT.

For a century, carmakers welded together steel and engineered physical parts. However, a new era of consumer technology, and rising competition from companies such as Apple and Google that take an interest in the industry, has forced carmakers to fill vehicles with software and code that can be compromised and with in-car connectivity that provides potential entry points.

> 'The more complexity you add to a system, the more vulnerable it becomes'

More than 100m cars are expected to have some form of connectivity by 2025, according to research by EY, the consultancy.

The attraction to manufacturers is clear: revenues from connected cars are expected to reach $25bn by then, 10 times more than today.

Many carmakers provide as standard "black box" telematics systems that use a long-range wireless link to transmit information about the vehicle in real-time. Others have turned to applications such as those found on a mobile phone to allow drivers to add software to dashboards.

Electronically-controlled systems, such as "steer by wire", which replaces a physical link between the steering-wheel and the axle with electronic sensors and motors, are only going to become more common. So, too, are cars that can steer themselves.

Harthmuth Hoffmann, head of technology communications at Volkswagen, the world's second-largest carmaker by sales, says: "In interfacing to smartphones, and in coupling navigation and information systems with driver assistance systems via radio-based communication, the vehicle is being opened increasingly to external software."

Mr Hoffmann notes that: "This new openness could heighten the risk of cyber crime," adding that Volkswagen has various levels of security to prevent access to its cars.

Last July, Volkswagen won a court ruling blocking a University of Birmingham academic from publishing research that he said provided the start codes for cars manufactured by the company and which could be used by potential hackers.

Ebay case adds to concern as shoppers' details fall into the hands of criminals

Homing in: the attack against eBay is the latest breach at a US retailing website Charlie Bibby

Retail

Boardrooms sharpen their focus after a series of breaches, says *Andrea Felsted*

Retailers are rushing to shore up their defences against cyber criminals after hackers targeting eBay were able to access passwords, phone numbers, addresses and other personal data on the retail website.

The attack against eBay is the latest cyber security breach at a US retailing website, after the hacking of Target and Yahoo's email service.

In December, at the height of the holiday shopping season, thieves stole credit card data from up to 40m Target shoppers.

The Target theft was one of the biggest breaches of data security in the retail sector since TJX Companies – a discount chain that owns TJ Maxx in the US and TK Maxx in the UK – said in 2007 that it had fallen victim to criminals.

Tony Caine, European vice-president of enterprise security at Hewlett-Packard, says: "Retailers are a huge target for hackers seeking credit card information, and new threats are resulting in more complex attacks."

US retailers have come together in an attempt to strengthen their ability to deal with cyber attacks.

Brian Dunefsky, in the New York office of law firm Withers, describes this as the "centrepiece" of the efforts by US retailers to protect themselves against hackers.

The plan is principally an exercise in sharing information on the threat of an attack and exploring technology to protect the retailers' systems, particularly the implementation of chip and pin codes, something that is standard in the UK, but not common in the US.

According to Mr Caine: "Magnetic stripe technology – which is prevalent across the US on credit cards – presents a gaping and exploitable vulnerability. The problem is that in this day and age, it is just too easy for criminals to duplicate these magnets. As with the financial sector and others, there is no silver bullet that will solve the problem and the criminal gains often far exceed the cost of carrying out the attacks."

He adds that the UK has made great strides by introducing two-factor authentication with "chip and pin" credit cards – making it ever more difficult for malicious elements.

> 'Magnetic stripe technology presents a gaping and exploitable vulnerability'

"It's a step that other countries such as the US should take heed of," he says.

Retailers could learn from counterparts in the financial services industry, which has been in the vanguard of cyber security protections.

Mr Dunefsky says that in the US "the financial services and healthcare companies are regulated by the government. That is what pushed them to do a better job of securing their data. Retailers are not really under that regime."

However, Kenny Mullen, a partner in the technology team at Withers' London office, points out that in the UK, if retailers are handling any credit card data, they are subject to the payment card industry data security standard, which strongly recommends that retailers do not store any cardholder data themselves.

Another way that retailers are shoring up their defences is through insurance to protect them against losses from cyber criminals.

Stephen Wares, who heads insurance broker Marsh's cyber risk practice in Europe, the Middle East and Africa, says there has been a sharp rise in demand for cover from retailers. In fact, interest from retailers is ahead of all other types of companies.

"We have seen more retailers come to us asking for cyber insurance in the past few months," says Mr Wares.

He says that in the final six months of last year, Marsh's European cyber risk book increased by 80 per cent. "A lot of that was driven by retailers," he adds.

Over the past year, cyber risks have risen up the agenda for store groups.

"The conversations we are having with retailers now are quite different from the ones we were having a year ago," says Mr Wares.

"Then, we were talking about the concept of cyber insurance. We are now talking to them seriously about their approach to the insurance market and how much cover they have got. They are coming to us with the intention of securing firm sign-off for the premium spend to buy insurance."

Among the risks typically covered by a cyber insurance policy are the loss of personal information, including protection against class actions from consumers and banks, and regulatory action.

It also covers the costs associated with managing the crisis, notification obligations and the costs of credit monitoring, if someone is opening a line of credit in an individual's name.

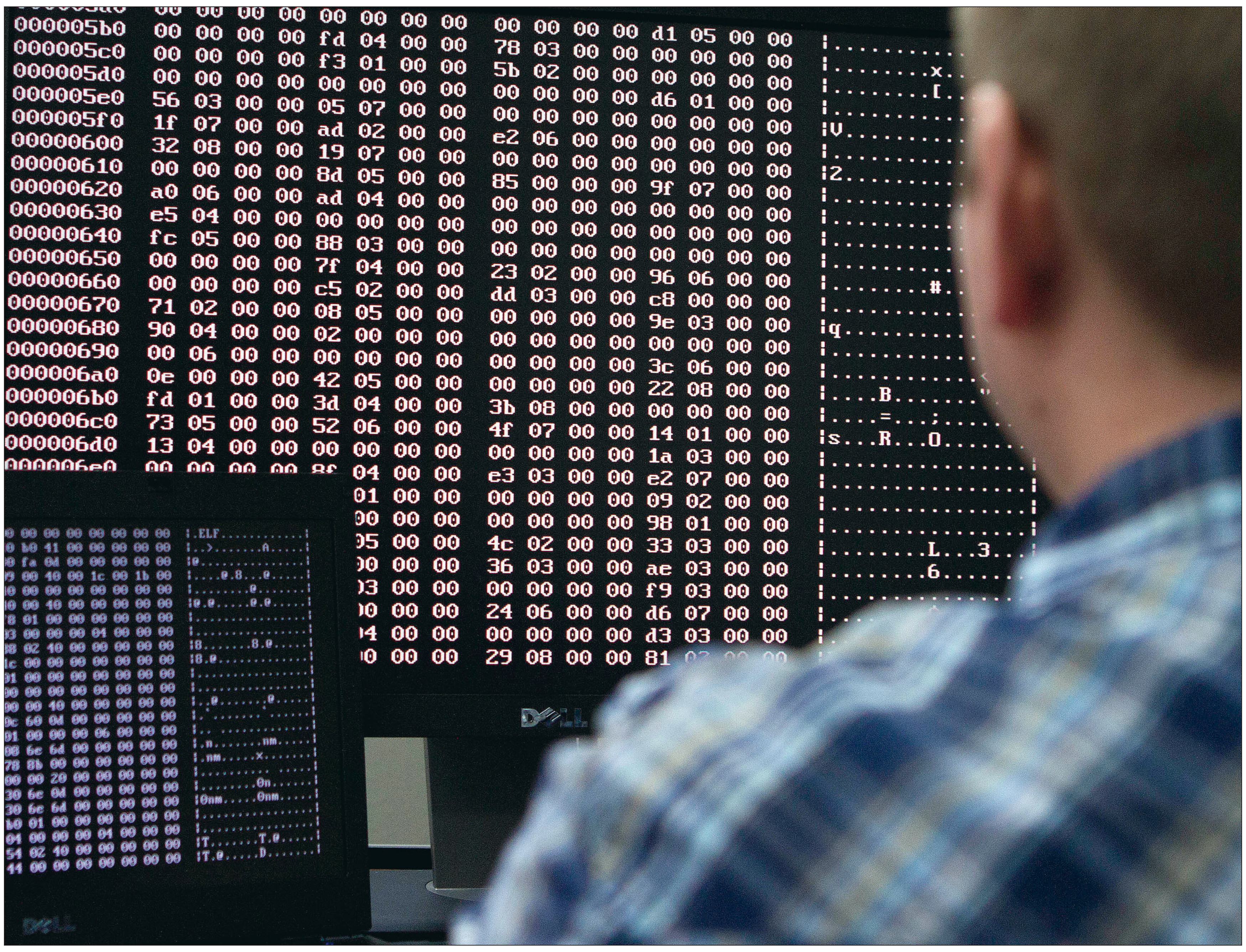
It is not just risk managers – whose job is to mitigate hazards in the organisation and buy insurance cover – who are becoming more concerned about cyber risks. Retailers' boards are also increasingly aware of the threats.

Target's management paid the price for the breach in the company's security, when its chief Gregg Steinhafel resigned in May.

"We see a lot more board level participation in the recognition of cyber as a risk and a demand from the board that the risk manager or insurance buyer explores the insurance market, to see if they can find a solution," says Mr Wares.

Energy makes prime target in threat against infrastructure

Industry The authorities are recognising the risks to vital public services, says *Neil Munshi*



Screening process: analysts say the industrial internet's safeguards are 'years behind'
Reuters

In May, the US Department of Homeland Security revealed that the industrial control system of a public utility had been hacked by a "sophisticated threat actor".

The department – or rather its industrial control systems cyber emergency response team (ICS-CERT) – did not reveal the type of utility. But access to the control system of a power company could give hackers the ability to switch off parts of the electrical grid, while access to a water utility's control system could allow them to interrupt water supplies.

In 2012, the agency said hackers had waged a campaign to break into the systems controlling US natural gas pipelines.

The method used on the utility was rudimentary: a "brute force" attack that compromised the system's remote access connection to the internet by trying a variety of password combinations.

High-profile data breaches such as the one that hit Target, a US retailer, in which the personal information of 70m people and the payment card data of 40m was compromised – dominate public discussion.

But companies and governments are increasingly focusing on the industrial internet. Analysts say it is years behind the security safeguards of the consumer-facing web and the consequences of a cyber attack could be much more damaging.

The targets are many: oil, gas and other energy systems, telecoms, manufacturing, transport, finance and public water, notes Slava Borilin, of security company Kaspersky Labs.

"In other words, everything that makes the modern world function," he says. "Just imagine a major city left with no water supply or a single working ATM or Point of Sale terminal just for a few days. It would be a disaster."

Meanwhile, "the internet of things" has taken over consumer electronics – washing machines, for instance, that are accessible via iPhone app. But oil rigs, manufacturing equipment and ships, to name a few, also "talk" to their administrators, rapidly transforming once largely closed networks into entities which have many points of contact with the broader internet.

That has increased efficiency and enabled real-time monitoring. But it has also made industry exponentially more vulnerable to threats from state actors looking to disrupt critical infrastructure, terrorists searching for targets, rivals hunting for trade secrets, disgruntled employees settling scores and activists hoping to make a point.

The US last month indicted five Chinese military officers, alleging they hacked into five US companies, including US Steel and Alcoa. The companies' general networks were compromised, but analysts say the damage could have been far greater had the industrial control system been hit.

The rush to connect has opened a "huge attack surface of software that is poorly written and has never really been securely tested", says David Chartier, chief of Codenomicon, which offers security testing services to makers of the software and sensors embedded in equipment, and to industrial companies that make or buy that equipment.

He says building firewalls is not enough. Hackers are exploiting vulnerabilities that are not publicly known, and which cannot be detected or blocked. "They can operate in a system for eight-to-12 months without being detected," says Mr Chartier. "Companies are compromised and don't even know it."

Cyber attacks on industrial control systems reported to ICS-CERT jumped from 34 in 2010 to 257 in 2013. That does not include the many intrusions that companies do not report – because of trade secrecy or the commercial implications of admitting to being compromised – or the many more that simply do not know they have been infiltrated.

It is important for companies to make thorough inventories of where their industrial systems connect to the general internet, or are otherwise exposed, and harden them against infiltration, he says. That will involve internal or external audits to find hidden vulnerabilities.

Hackers exploit such holes because "even the most basic security measures aren't being implemented," says Larry Zelvin, director of homeland security's national cybersecurity and communications integration centre.

Hackers "are jumping over a one-foot fence". He recently told an SEC conference that a US water utility had been the victim of "a very significant cyber attack that emanated from the other side of the globe".

Energy is an obvious battleground. The Stuxnet computer worm attack impaired Iranian uranium centrifuges in 2010. The 2012 attacks on Saudi Aramco and Qatar's RasGas aimed to stall production and occurred within days of each other. Some 30,000 Aramco computers were compromised. If an industrial systems administrator's personal computer or mobile were hit, it could open the way to the pumps, valves and junction boxes of the system concerned.

All industries are vulnerable, says Brian Ahern, the chief of Lockheed Martin Industrial Defender, a security company.

"This is the new normal," he says. "We're going to see an exponential increase of intelligent devices, all the way down to people's homes. That's just opening up the apertures and the various ways the actors can gain access to critical infrastructure."

'We are going to see an exponential increase of intelligent devices'

High-profile hacking increases pressure to respond to public fears

Continued from Page 1

In the China case, Washington has surprised many with its public warning to Beijing. The justice department alleged that the officers hacked into the computer systems of five US steel companies and a labour union to steal secrets.

Eric Holder, attorney-general, pointed to a unit of the People's Liberation Army in Shanghai. Previously, the US government has tended to speak in broad terms about cyber threats. Unusually, he named the companies that had been the victims of the alleged intellectual property theft.

The Wanted posters raised awareness of a threat but the chance of arresting the officers or halting any cyber espionage programme is slim. China hit back, calling the US a "high-level hooligan", and announced a new security screening process for foreign IT products and services.

Cyber criminals in the US face heightened attention from law enforcers.

In May, the FBI arrested hackers who allegedly used a "sophisticated and pernicious" form of malware. At $40, the Blackshade remote access tool, says Preetinder Bharara, US Attorney for the Southern District of New York working on the case, is "inexpensive and simple to use" but with "breathtaking" invasiveness, including the ability to spy on people using their web cameras and log their keystrokes.

The FBI were able to arrest Brendan Johnston, who was allegedly paid to help sell malware including Blackshade, and two people alleged to have bought the software and used it to steal online account information.

In a rare victory for cross-border cyber crime co-operation, Alex Yucel, alleged co-developer and head of a group selling Blackshade, was arrested in Moldova last year and awaits extradition to the US.

These moves are the first steps of a fightback against a still growing threat.

Stuart McClure, founder of cyber security company Cylance, says the very definition of a cyber criminal has changed in recent years: "It used to be kids in the basement, then it moved to organised groups such as Anonymous [the hacking activist association] in the early stage, then more organised crime, targeted espionage and then nation states."

Protections against hackers remain conspicuously weak, what with security software that turns out to be hugely flawed and a skills shortage that makes cyber security specialists too expensive for many companies and state and local governments to hire.

The discovery of the "Heartbleed" bug in April highlighted quite how under-resourced cyber security has been. The flaw in Open SSL, better known as the software behind the little padlock image that indicates a web page is secure, left two-thirds of the world's websites vulnerable to cyber attack.

Hackers were able to exploit the flaw to request anything in a computer's short term memory, from passwords to data such as social security numbers stolen from Canada's tax authority.

Open SSL, a vital plank of security, which was even used by large technology companies including Google and Yahoo, was severely underfunded and maintained by the equivalent of just two full time software engineers.

The project to develop Open SSL was set up in the late 1990s as a non-profit foundation. It received less than $2,000 in donations a year until the flaw was unearthed, prompting the tech industry to pledge almost $3m to secure the software and other core infrastructure.

The shortage of cyber security skills makes defence difficult even for organisations with larger budgets. In the US, 200,000 software security positions are unfilled, with a particular shortage of experts in network security, according to the Boston Consulting Group.

The targets rich with confidential data that can be sold on the thriving black market are not necessarily those able to lure the best security engineers. State and local government, universities and small businesses, for example, struggle to recruit the talent they need.

Law enforcement sorely lacks an international framework to help with cross-border investigations and prosecutions.

Mr McClure says: "Interpol, God love them, I know a lot of guys there try really hard, but there are no universal laws, no Geneva pact for cyber war and engagement, no cross-boundary or -nation laws.

"There probably needs to be a 100-fold increase in what law enforcement authorities are doing. They just don't have the bandwidth, the resources, to do that."

Contributors »

Hannah Kuchler
San Francisco correspondent

Sam Jones
Defence and security editor

Henry Foy
Motor industry correspondent

Andrea Felsted
Senior retail correspondent

Neil Munshi
Chicago & Midwest correspondent

Simon Mundy
Seoul correspondent

Alistair Gray
Insurance correspondent

Peter Chapman
Commissioning editor

Andy Mears
Picture editor

Steven Bird
Designer

For advertising, contact:
Liam Sweeney,
on +44 (0)20 7873 4148,
Liam.Sweeney@ft.com, or
your usual FT representative.

All FT Reports are available
on FT.com at ft.com/reports

Follow us on Twitter at:
@ftreports

Seoul suffers from poor web controls

South Korea

A country proud of its leading position in the digital world has a curious blind spot on internet safety, writes *Simon Mundy*

South Koreans are the envy of computer geeks around the world for having the fastest average internet speed on the planet – more than double that of the US. Yet internet users have to contend with a cumbersome, dated security system that is blamed for hindering ecommerce and innovation – and also, paradoxically, undermining internet security.

By law, anyone using online banking in South Korea must use a "digital certificate" issued by a bank. This process requires an ActiveX plug-in, an outdated technology developed by Microsoft that is broadly ignored by web developers outside South Korea and is incompatible with internet browsers except Microsoft's unfashionable Internet Explorer.

Thus, South Korea holds another world record. It is the only country where Internet Explorer accounts for more than half the browser market. Research site StatCounter says 76 per cent of South Koreans use the Microsoft browser instead of faster, more reliable browsers developed by the likes of Google and Mozilla.

This has created a self-perpetuating cycle where many South Korean web developers focus only on building sites compatible with Internet Explorer. Users of other browsers find that many South Korean websites – including the local sites of foreign groups such as Standard Chartered and Citibank – do not function properly.

Reliance on Internet Explorer was a source of alarm in April, when the US government advised citizens to avoid using the browser, after it was discovered that a programme flaw could allow hackers to steal personal data.

Microsoft fixed that problem but even it advises users to shun the ActiveX technology, where possible.

Microsoft admits on its website that ActiveX controls can "pose a security risk" and says: "It's best to avoid using them if the website will work without them. They can stop your computer from functioning correctly, collect your browsing habits and personal information without your knowledge." It adds: "Also, 'good' ActiveX controls might contain unintended code that allows 'bad' websites to use them."

Computer says no: South Koreans have to use slow and outdated browsers Alamy

South Korean internet experts say the vulnerability of ActiveX is one of the main reasons for the high rate of hacking and data leaks in South Korea.

Internet users have to download so many plug-ins when web surfing, that malicious ones can easily slip through. A high-profile incident last year saw systems brought down at several broadcasters and financial institutions in an attack attributed by the government to North Korean agents.

Media reports said the hackers had exploited ActiveX, although investigators said this could not be proven.

"Because of ActiveX, Korea has become a number one place for hackers," says Lee Min-wha, a professor at the Korea Advanced Institute of Science and Technology. "South Korean internet users are trained to click 'yes' to everything."

The system was initially an object of pride for the South Korean government, which saw it as proof of the country's move towards the technological cutting edge.

In 1998, the authorities deemed the available online payment systems too insecure. The new SSL protocol had not been authorised for export from the US. As other countries waited for SSL, South Korea developed its own system, SEED, which can be used only with ActiveX plug-ins.

For years, regulators and card operators resisted calls to change the system, deterred by fears of the disruption that a new model would cause, and of security risks that could be caused if it were implemented badly.

This year, the government is at last promising change, with public frustration having reached new highs.

A survey, by the Federation of Korean Industries, a lobby group, found that 84 per cent of respondents wanted a new system. The burdensome old one is blamed for holding back the development of ecommerce.

It has also protected local personal computer makers Samsung Electronics and LG Electronics against Apple, whose Mac computers account for just 1.7 per cent of the South Korean PC market, compared with 8.9 per cent globally, according to StatCounter.

President Park Geun-hye intervened when she heard of the frustration of Chinese fans of a South Korean soap opera, who could not buy associated merchandise because of the security controls. As a result, digital certificates will not be required for online transactions from June.

No plans exist to change the system for online banking. Moreover, any change to the ecommerce payment systems needs support from South Korean card companies. This may not be forthcoming, warns Lee Dong-hwan, information officer of Paygate, an alternative payment system that has been shunned by card operators despite interest from online retailers.

"Tests showed that satisfaction levels with our product were five times higher than for ActiveX," Mr Lee says. "It would provide benefits for merchants and customers, but the card companies would have to change their existing security frameworks."

State and local bodies lack defences

Government

More resources are needed to protect plum targets, says *Hannah Kuchler*

Cyber criminals on the hunt for poorly protected confidential data are circumventing the US federal government and targeting state and regional authorities on the basis that they have fewer resources to defend themselves.

Social security numbers, driving licence numbers and home addresses are among the data kept by government now that access to local services is moving increasingly online.

More than two-thirds of US government data breaches were at non-federal agencies in 2012, the latest year that data were available from the US computer emergency response team.

Computer security incidents rose 42 per cent in the US regions and provinces compared with a rise of only 5 per cent overall.

Wade Williamson, senior threat researcher at the Google Ventures-backed security start-up, Shape Security, says that given the large amount of sensitive information they hold, state government agencies are "really enticing targets".

He says that hacktivists – who attack for publicity – had often chosen them as targets, because they are highly visible in the media and do not have anywhere near the budgets or personnel of federal government.

"Hackers can expose a bunch of personal information and post it out there to show 'we broke into a site'. It is going to gain them notoriety," he says.

"We've seen this quite a bit all the way down to individual towns' police forces that are hacked as soft targets."

Groups affiliated with Anonymous, a loosely knit hacking activist association, have explicitly targeted local government. This includes a campaign against the Los Angeles police department and a contractor that builds websites for sheriff's agencies across the US.

The financial benefits of stealing data are alluring. Personal information can be sold on the black market, even if it does not include credit card details.

Cyber criminals stole social security numbers of up to 280,000 people when they broke into the Utah state government servers in 2012. Hackers may have obtained up to 160,000 numbers and 1m driving licence numbers after an attack in Washington state last year.

Meanwhile, South Carolina blamed an "international hacker" for an incident that affected more than three-quarters of the state's 4.6m population.

This year, according to Privacy Rights, a group that collects information on data breaches, this year, the California driving licence authority has investigated a potential breach of card data, while the city of Detroit has reported the exposure of information related to almost 2,000 current and former employees.

With small teams, often composed of fewer than five people, state governments find it difficult to secure data.

A survey of chief information security officers of US states, counties, cities and towns last year reported almost half as saying their IT infrastructure was not prepared for an attack, according to Consero, a Maryland-based company that runs forums for executives.

Mr Williamson says even if state and local government were to increase their cyber security budgets, they would struggle to recruit skilled security engineers in a very competitive market.

"They have a really hard time holding on to their people, so it is important for them to look at a solution that minimises how much human interaction it requires," he says.

"They can't have a new product that needs two PhDs to run the thing, as they might not have the talent in-house."

Some 86 per cent of chief information security officers in state government agencies say a lack of sufficient funding is the main barrier to addressing cyber security problems.

Half manage a team of fewer than five, according to a 2012 survey by Deloitte and the National Association of State Chief Information Officers.

States may handle large sums of money, comparable to those managed by Fortune 500 companies, but they have far fewer cyber security staff. Most financial institutions employ more than 100 people in their security operations.

On average, cyber security only receives 1 to 2 per cent of a state's overall technology budget and, unlike in the private sector, this does not appear to be rising.

'We have seen this all the way down to individual town police forces that are hacked'

Srini Subramanian, who leads Deloitte's cyber risk services practice for state and local governments, says that five or six years ago most data breaches were inadvertent; for example, an official might have lost a laptop. In the past couple of years, states had begun to be subjected to sophisticated attacks.

Mr Subramanian says state government bodies are more vulnerable because they are not subject to the strict regulations that federal agencies submit to, or, if they are – in the case of agencies handling tax data or health information – the laws are not enforced.

"The federal agencies do these assessments [on state bodies] more as safeguards, to give feedback. They seldom result in penalties or immediate impact, such as the connection to the federal agency being terminated," he says.

Darktrace aims to safeguard the private sector

Intelligence

Ex-GCHQ man says business has to look for the 'unknown unknowns', writes *Hannah Kuchler*

It was Andrew France's frustration with the "professional undertakers" of the cyber security industry that pushed him to end a 30-year career with the UK intelligence services last summer.

The chief executive of Darktrace, a Cambridge-based cyber security start-up, was the deputy director for cyber defence operations at GCHQ when he quit to join a company that he hopes will shake up the private sector response to cyber crime.

Seeing the number of attacks rising, the online criminals becoming more sophisticated, and the consequences encroaching further into the lives of ordinary people, he thought the industry was failing.

It always responds to the last threat rather than anticipating the next one, he says.

"For many years, I was frustrated with the security industry. They've all got hammers so every problem is a nail. The whole approach was a bit like being professional undertakers, who didn't get involved until the bad stuff happened and then enjoyed high fives all round when the mess was tidied up," he explains.

Some cyber security companies do specialise in clearing up the mess after an attack, but more and more are working to detect threats. Yet, often they scan company computer systems looking for potential problems that are on a list of already known threats, or have computer programmes that follow set rules to look for attackers.

This approach does not necessarily discover today's cyber criminals, who are quickly chopping and changing their techniques to stay under the radar.

Mr France warns that this lulls these companies' customers into a false sense of security.

A team of former government cyber defence leaders teamed up with mathematicians at the University of Cambridge to create Darktrace, which uses an advanced technology that helps monitor patterns across a company's computer network, map what is normal activity, and spot abnormalities.

"Using a computer is like driving a car. Different people will use it in a slightly different way. In a car, you may listen to a different radio station, accelerate differently, brake differently," Mr France notes.

"We have built a set of algorithms that mathematically analyse whether the someone driving hasn't driven it before."

The Darktrace cyber intelligence platform works to detect "unknown unknowns" rather than definite cyber breaches. It can alert IT staff to potentially troubling activity.

The company is one of a new generation of cyber security start-ups that aims to adopt a different approach to detecting hackers from that first developed by antivirus software makers.

Darktrace's Andrew France

Many are based in Silicon Valley, with a handful in Israel. Darktrace is one of the only UK-headquartered cyber security companies. It also has offices in Paris and Milan.

After launching its sales operation last year, it has customers in retail, manufacturing and national infrastructure. "It has gone like a rocket because of the uniqueness of the approach," Mr France says.

In February, it won a contract with Drax, the UK's largest power station, which provides about 7 per cent of the country's electricity needs. Critical infrastructure bodies such as power companies are waking up to the need for greater protection from cyber criminals, who could run rampant if they seized control of key computer networks (*see page 3*).

Martin Sloan, Drax head of safety and security, has said that the Darktrace system has already identified threats with the potential to disrupt Drax networks.

Darktrace is backed by Invoke Capital, the venture capital firm founded by Mike Lynch, former chief executive of Autonomy, the software company bought by Hewlett-Packard in a controversial $11bn deal in 2011.

Mr France says the British funding would mean that the company would not be sold to Silicon Valley, which he criticised for buying ideas and killing them.

Mr France spent the last years of his GCHQ career developing a national cyber defence strategy, as part of a mission to protect British intellectual property from foreign cyber spies.

Other executives, including Steve Huxter, chief operating officer, and John Richardson OBE, director of security, also had long careers working on cyber defence for the government.

The UK government set aside money with the aim of making Britain one of the most secure places to do business online, protecting British interests in cyberspace and, in the UK, improving cyber security skills, a resource in global short supply.

Mr France sees Darktrace as continuing that by leading a private sector push to defend British assets.

"The treasure of the UK is in the data it holds," he says. "We have trusted financial brokerages, trusted networks. This is an economic issue not just a security issue."

Target's costly Christmas fiasco strengthens the case for cover

Insurance

Data losses point to need for widening of market in which US is way ahead, writes *Alistair Gray*

Bad though it was, it could have been worse. Target is still counting the cost of Christmas, when hackers broke in to the US retailer's systems and stole payment card data of 40m customers.

The debacle has cost the discount chain at least $18m. But Target would have lost almost half as much again were it not for its insurance, which triggered $8m in payouts.

With Sony, Vodafone and others also having suffered attacks, it is no wonder executives are turning to insurance to confront IT-related risks.

"A lot of people are realising it's a must-have," says Paul Bantick, cyber insurance specialist at Lloyd's of London insurer Beazley. "It's impossible to obtain 100 per cent security. It's a question of when, not if.

"Management look at every high-profile breach and say: 'We need to be protecting ourselves'." Underwriters have been developing IT-related policies, while increasingly excluding the associated risks from traditional insurance that could otherwise pay out, such as professional liability or property cover.

From near non-existence at the turn of the century, the US market for cyber insurance has grown by about 30 per cent a year recently. However, it remains much smaller than more established lines of insurance.

The US dominates. An estimated quarter of US companies have some cyber coverage. Take-up is prevalent among larger groups, consumer-facing companies such as retailers, or those that store large amounts of personal data, such as financial institutions and healthcare specialists.

The industry is estimated to write about $1.3bn worth of cyber premiums a year. Brokers say the market in Europe is only about a 10th of that.

This is in large part because several US states have laws demanding organisations tell customers when their data has been lost or stolen, putting companies at risk of law suits.

"That's been the driver in the US," says Stephen Wares, head of Europe, Middle East and Africa cyber liability for insurance brokers Marsh. "We haven't had that in Europe."

That may be about to change. EU officials are updating online data privacy rules, expected to be implemented in about three years. Details are being debated but policy makers are set to introduce stringent penalties for breaches, possibly involving fines as high as 5 per cent of global turnover. Organisations will also be required to inform customers.

"That will be the catalyst," says Sarah Stephens, head of cyber insurance in Europe for brokers Aon. "We may not see law suits such as have been in the US," but if customer data are compromised the rules "will still expect companies to do certain things".

For now, much of the cyber insurance market focuses on personal data breaches. Such policies cover a wide range of expenses, from public relations and customer notification, to law suit defence and IT forensics.

The bill could have a substantial impact on profit and loss accounts. Yet other consequences of cyber attacks, such as network downtime or supply chain disruption, might be more serious. But insurance against non-data-related incidents remains.

This is partly because the industry lacks the claims data it has built up in more than a decade of personal data breaches. This makes losses from other cyber-related risks harder to assess, and harder to price.

'If companies don't regard it as a board level issue, I don't know what it will take'

Whereas big corporate insurance buyers can secure up to $400m of protection for data breaches, the limits of cyber-related business interruption policies tend to be about half this level, brokers say.

Demand is also not as high as it is for privacy-breach cover. "When a law is passed and you're mandated to do something, that clearly focuses your mind," says Mr Wares. In other areas, the need for IT insurance "has perhaps been less obvious," he adds. "But that is changing."

Brokers say insurers are devising policies that cover a wider range of IT threats and, says Ms Stephens, increasing take-up of data breach cover could encourage more cyber insurance.

Axel Lehmann, chief risk officer at Zurich, says concerns about cyber risks are no longer the preserve of the IT guys in the basement. They have reached top management level.

The Target case shows cyber attacks can have a significant financial impact. The retailer's chief, Gregg Steinhafel, resigned five months after the Christmas fiasco.

Now, says Aon's Ms Stephens, "if companies don't regard it as a board level issue, I don't know what it will take."