FT SPECIAL REPORT

Cyber Security

Friday April 10 2015

www.ft.com/reports | @ftreports

At war with an invisible enemy

The US president has ratcheted up the rhetoric, but how can cyber threats be fought, asks *Hannah Kuchler*

Illustration: Oivind Hovland

When President Obama stepped up to the podium to give his annual State of the Union speech in January, he gave cyber security experts a glimmer of hope that their fears of massive harm were finally being considered as a great threat to the nation.

Sandwiched between comments on diplomacy in Iran and the Ebola epidemic, the President said that if the US government did not act to improve cyber defences, "we'll leave our nation and our economy vulnerable".

"No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets or invade the privacy of American families, especially our kids," he said to applause.

Then, last week, Mr Obama ratcheted up his response, declaring foreign cyber threats a "national emergency" and taking action to pave the way for sanctions against those who engage in cyber attacks that endanger America's national security or economy.

His executive order gives the government new powers to target significant cyber threats that affect critical infrastructure, disrupt the availability of websites or networks or steal trade secrets and financial information, such as credit card data.

Cyber criminals could face new potential punishments including having any US bank accounts or other assets frozen and banning US entities or people from doing business with them.

But legislating against hackers is difficult. As cyber attacks hit companies from Sony Pictures to US retailer Home Depot and cyber criminals infiltrate IT networks and countries, lawmakers struggle to keep up and find ways to limit the damage they cause.

Corporations are desperate for support against the fast-changing threat but, so far, many feel they must rely on private cyber security companies rather than government or law enforcement.

This report shows the scale of the problem. Kris Lovejoy, IBM's chief information security officer, argues it should be compared to "biological warfare". Speaking at a cyber security conference in Israel, as our Jerusalem correspondent writes (*see page 4*), she said: "Everyone is infected — everyone — [and] the bad guys are in our organisation."

The answer lies not only in technological solutions, which government often finds difficult to implement, but also in people and processes, cyber experts argue throughout this report.

Amit Mital, chief technology officer at Symantec, the internet security company, says in the article on payments (ft.com/cyber-security) that people are often the weakest link. This is backed by David Emm, principal security researcher at Kaspersky Lab, the software security group, who is quoted in the article on authentication (*page 2*), arguing that passwords are usually breached because of human weakness, not sophisticated technologies.

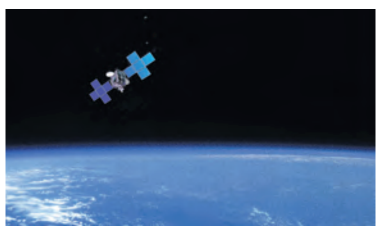
Talking tough: Barack Obama last week declared overseas cyber threats a 'national emergency'

Tony Cole, global government chief technology officer at FireEye, a New York-listed cyber security company, says people need to change how they think of cyber attacks.

"The biggest thing people need to understand is we don't have a malware problem, we have an adversary problem," he says. "Adversaries are always looking for new holes and there are hundreds of millions of lines of code in everything we have out there."

Continued on page 4

Inside



On FT.com
New payment methods raise security concerns
ft.com/cyber-security

Online threat is growing as global tensions increase

Geopolitical risk

Conflicts between states look increasingly likely to be played out in the virtual world, writes *Sam Jones*

Geopolitical risks used to be something that only companies with a global presence had to worry about. But in cyberspace, any connected modern business is vulnerable.

It is no longer enough for companies to sever ties with unsettled regions, cut loose risky subsidiaries or hedge their global exposures to manage their way through shifting international tensions.

The past two years — marked by the escalation of state-on-state disputes and conflicts — have shown that the effects of cyber warfare or aggression can be experienced by almost any business.

Companies can be victims of state-sponsored attacks for strategic reasons unconnected with their immediate business, from filmmakers such as Sony Pictures — allegedly hit by North Korean hackers last year — to Spanish renewable energy companies, targeted by Russia-linked hackers.

The nature and motivation for attacks is varied: from classic state surveillance to economic espionage, criminal gain, embarrassment or destruction.

"Whenever we have discovered a new domain in the history of mankind, we have had conflict over it," says Dave DeWalt, chief executive of FireEye, one of the world's biggest cyber security companies.

He believes such conflict in cyber space is already upon us: "We are seeing more and more complex attacks — highly sophisticated operations. On average, we are seeing attackers inside their target's networks for about 200 days before they are discovered."

Many western security officials fear that, as conflicts heat up around the world, cyber will become the front line for more overt, aggressive attacks.

With many of the world's disputes deadlocked — the stand-offs between Iran and Saudi Arabia, North Korea and South Korea, Japan and China, or Russia and Europe — cyber is likely to supplant the physical world as the main theatre of conflict.

"There is a correlation between cyber attacks with the rise of geopolitical tension," says Christophe Birkeland, chief technology officer of malware analysis at Blue Coat, a cyber security company. Cyber attacks are following the pattern of other kinds of advanced arms proliferation, he believes.

"Once the new weaponry is used successfully, all the ambitious would-be up-and-comers . . . follow suit," he says.

According to PwC, the professional services company, the number of cyber security incidents reported in 2014 by large businesses increased globally by 48 per cent to 42.8m — the largest jump in attacks since 2010. Of almost 10,000 organisations and individuals polled by PwC worldwide, nearly one in 10 reported breaches costing their business a total of more than $10m annually.

The nature of cyber threats differs by region. The focus of Chinese hacking is intellectual property theft, while Russian activity is driven by espionage, vandalism and criminality. For the US or Britain, activities have centred on surveillance and the hacking of telecommunications.

Many believe that tensions in the Middle East are the likeliest to lead to a flashpoint in the digital domain in the near future. "The number of cyber attacks from Iran directed against Saudi Arabia and the US is growing," says Stuart Poole-Robb, head of the KCS corporate intelligence and security group.

Name and shame: Dave DeWalt of FireEye wants to embarrass attackers

He points to the virus that infected Saudi state oil company Aramco's IT system in 2012, erasing data on three-quarters of PCs, replacing emails, spreadsheets and documents with an image of the US flag in flames.

"Hackers . . . claiming to be upset about Saudi policies in the Middle East were traced to Iran by US intelligence," says Mr Poole-Robb.

With the prospect of a nuclear detente between Iran and the west, growing Israeli concern about Tehran's ambitions, and a fully fledged proxy war between Saudi Arabia and Iran in Yemen developing, many see the first fully destructive cyber attacks — including, possibly, the first to cause harm to humans — as likely to emerge in the region.

Against such a backdrop, the main issue is one of enforcement and deterrence. Some companies are even talking about the possibility of having retaliatory capabilities.

"I see a lot of talk about that and a desire to do it," says Mr DeWalt. "But when it comes to it, it's like going into a fight with a peashooter."

Ultimately, Mr DeWalt says, the best weapon for large businesses in cyberspace could be "the embarrassment variable" — naming and shaming attackers, particularly states. It might not seem a powerful tool in a world of international cyber aggression, bullying and war, but it might be the best option available.

Customers become less tolerant of flawed and vulnerable code

Software design

Lack of industry standards and legal frameworks leaves products open to criticism, writes *Jessica Twentyman*

In December 2014, Google released information about a vulnerability that researchers working on its Project Zero bug-hunting initiative had discovered in Microsoft's Windows 8.1 operating system. Google had raised the issue privately with Microsoft three months previously, but Microsoft had failed to address the issue within Project Zero's 90-day deadline.

Microsoft's response was swift and indignant. Chris Betz, senior director of Microsoft's Security Response Centre, took to the company's blog to chastise Google for the disclosure, made two days before Microsoft was due to release a patch for the vulnerability.

He acknowledged that Microsoft has a responsibility to protect customers — but said that software vendors needed time to prepare patches.

"Let's face it, no software is perfect," he wrote. "It is, after all, made by human beings."

Customer sympathy may be wearing thin, however. Cyber criminals have never been more proficient at taking advantage of weaknesses.

Corporate IT security teams, meanwhile, are trapped in a desperate race, devoting time and money applying security patches to fend off attacks. Many are starting to question whether the responsibility for fixing software should be theirs at all.

"There are too many updates and they arrive too frequently. It's annoying and worrying for businesses," says Rolf von Roessing, international vice-president of Isaca, a worldwide association of security professionals.

"Software vendors bring these products into the world with all their vulnerabilities, but it's the companies that buy them that are left dealing with the consequences."

At last year's Black Hat IT security conference in Las Vegas, a similar point was made by Dan Geer, chief information security officer at the CIA's venture capital arm, In-Q-Tel. He argued for legal measures to push much of the accountability for security back on to the companies that develop vulnerable code, in order to protect customers who, today, have no legal recourse if negligent coding exposes their systems to danger.

But in the absence of an effective legal framework in the US or elsewhere, the debate rumbles on.

Dave Merkel, chief technology officer at FireEye, an IT security vendor, urges business leaders to accept software vulnerabilities as a fact of life. "Attackers are specifically looking for the things that code was not designed to do. As a software creator, you can test definitively for all the things that your software should do. But testing it for all things it shouldn't do is an infinite, impossible challenge," he says.

The problem is compounded by the fact that software products evolve. Anthony Hess, senior manager of the cyber security group at KPMG, the consultancy, points out that new releases are issued and new functionality is built on top of the original code. These changes can push the original design to its limits, but most vendors are reluctant to change the base code of older products.

Call for legal change: Dan Geer of In-Q-Tel, the CIA's venture capital arm

The cost of rebuilding software from scratch would almost certainly be passed on to customers in any case.

In addition, the original design of most enterprise software products is unlikely to have been conceived with any specific, widely understood standard in mind, adds Wolfgang Kandek, chief technology officer at Qualys, another IT security vendor.

"Building software isn't like building a house or a bridge or a ship, where accepted engineering principles apply across whole industries. In this respect, the software industry has something of a maturity problem," he says.

It is this lack of design standards that the Center for Secure Design (CSD), a working group set up last year by the IEEE Computer Society, an organisation of computing professionals, aims to address, according to steering committee member Gary McGraw, chief technology officer of Cigital, a software security consulting firm.

"When it comes to software security, there's been too big a focus on bugs in code and too little focus on flaws in design — but we believe design flaws account for around half of IT security problems," he says.

The idea behind the CSD was to gather a group of the world's best software architects to come up with ideas to address these design flaws. That led to last year's publication of the CSD's paper, "Avoiding the Top 10 Security Design Flaws".

Now, says Mr McGraw, the group is looking at how to apply this advice to specific application development frameworks and to specific industries.

"We have to build better software," he says, "because we can't go on protecting software from all the attackers out there by putting a barrier, or patch, between broken software and bad people."

Finding fault becomes a lucrative business

Bug bounties Tech companies will pay tidy sums to those who spot holes in their defences, writes *Murad Ahmed*

Concerned about protecting the personal and financial details of its users, PayPal, the online payments company, has introduced a system called "two-factor authentication".

To log in, users must first enter their user name and password. They then receive a security code by mobile phone that they have to type in to gain entry. The idea is to create an extra barrier that makes it harder for criminals to break into a customer's account.

The only problem was that this additional line of defence had a significant flaw. Last year, a group of computer hackers from Duo Security, a Michigan-based cyber security company, discovered a problem with PayPal's mobile app that meant it was possible to bypass this second barrier because of a previously unknown bug in PayPal's systems.

Zach Lanier, senior security researcher at Duo, says users could have been "lulled into a false sense of security, unaware that a security feature isn't living up to its promise".

It was lucky for PayPal that it was Mr Lanier's team that discovered the problem. He was able to warn the company through its "bug bounty" programme, which pays people who discover security vulnerabilities. Duo Security pocketed the bounty while PayPal fixed the bug before revealing publicly how it been discovered.

Google, Mozilla and Hewlett-Packard are among other technology groups that have bug bounty programmes. Bounties range from $500 for spotting tiny bugs to $60,000 for uncovering serious flaws.

Millions of dollars have been paid to individual hackers and security companies through these schemes. Unveiling Facebook's bug bounty programme in 2011, Joe Sullivan, the social network's chief security officer, wrote on the company's website: "We realise . . . that there are many talented and well intentioned security experts around the world who don't work for Facebook. We established this bug bounty programme in an effort to recognise and reward these individuals for their good work and encourage others to join."

In 2014, Facebook paid $1.3m to hackers for their benevolence.

There is no way for companies to create perfect online defences. Underlying every website or app are lines of code. As these have been written by humans, defences can range from the well constructed to the sloppy and flawed.

In theory, thanks to bug bounties, some hackers can make a decent living just looking for security flaws. However, most who participate in the programmes are computer professionals who uncover bugs in their spare time to make some extra cash, or they stumble across problems by chance.

But approaching a company about any access flaws or bugs you find is not always a good idea. In 2011, Patrick Webster, a security researcher, found a problem at First State Super, an Australian investment group that allegedly left millions of customer accounts at risk. When he told it of the problem, the company reported him to the police. (Both police and civil actions were later dropped.)

Still, bug bounty programmes have become so popular among big technology companies that start-ups are emerging around what is becoming a lucrative industry. Last year, HackerOne, a cyber security company started by Alex Rice, who formerly ran the product security team at Facebook, raised $9m in funding from Benchmark Capital, a leading Silicon Valley venture capital firm.

The start-up is developing a software platform through which people can report bugs to companies and be paid for reporting flaws while at the same time avoiding unwanted attention from law enforcement. HackerOne has so far facilitated more than $1m in payments for about 4,000 reported bugs.

Explaining its motives, the company says: "There is a disturbing lack of trust and consistency relating to how people report vulnerabilities and how organisations respond to them . . . we're convinced that we must dramatically change how the world handles security research if we have any hope of advancing the state of security. We built HackerOne to empower the world to build a safer internet."

Bugcrowd is another company that wants to become a central repository for reporting flaws. In March, the company, which acts as a crowdsourcing platform for security researchers, announced it had raised $6m in funding from investors. In total, Bugcrowd has raised $9m since its founding in 2012, with companies including Western Union, a US financial services group, launching bug bounty programmes through its site.

Given the apparent success of programmes, some, such as Brian Krebs, a cyber security expert and blogger, have even suggested bug bounty programmes should be compulsory, with all companies forced to pay when security problems are brought to their attention. The idea is that this would create vast security improvements across the internet.

But others have warned that such programmes might not be right for all companies.

Chris Wysopal, chief technology officer at Veracode, a Boston-based online security company, says organisations should not attempt to create bug bounty programmes unless they have their own strong team of hackers to respond to any problems that are discovered.

After all, the only thing worse than being shown a hole in your online defences is the inability to close it.

Zach Lanier was able to warn PayPal through its bug bounty programme

Global satellite industry must invest in safety

OPINION

Jill Stuart

In 2007 the Sri Lankan government noticed that propaganda for the Tamil Tigers, the rebel group, was being broadcast regionally from an Intelsat satellite over the Indian Ocean.

This was not an unconventional business arrangement between the US satellite communications company and the rebels, but the result of a cyber attack. Two years earlier, Tamil fighters had hacked the satellite and proceeded to use its signal sporadically for their own political purposes.

Events targeting satellites are not isolated and they are likely to increase. The industry needs to spend money on security, to avoid both potential larger financial loss and threats to safety.

There are some 1,000 functioning satellites orbiting the Earth relaying and amplifying information sent through radio frequencies from one point on Earth to another. They form part of the infrastructure that we rely on for safety and quality of life.

Many people do not realise how pervasive satellite services are in contemporary society.

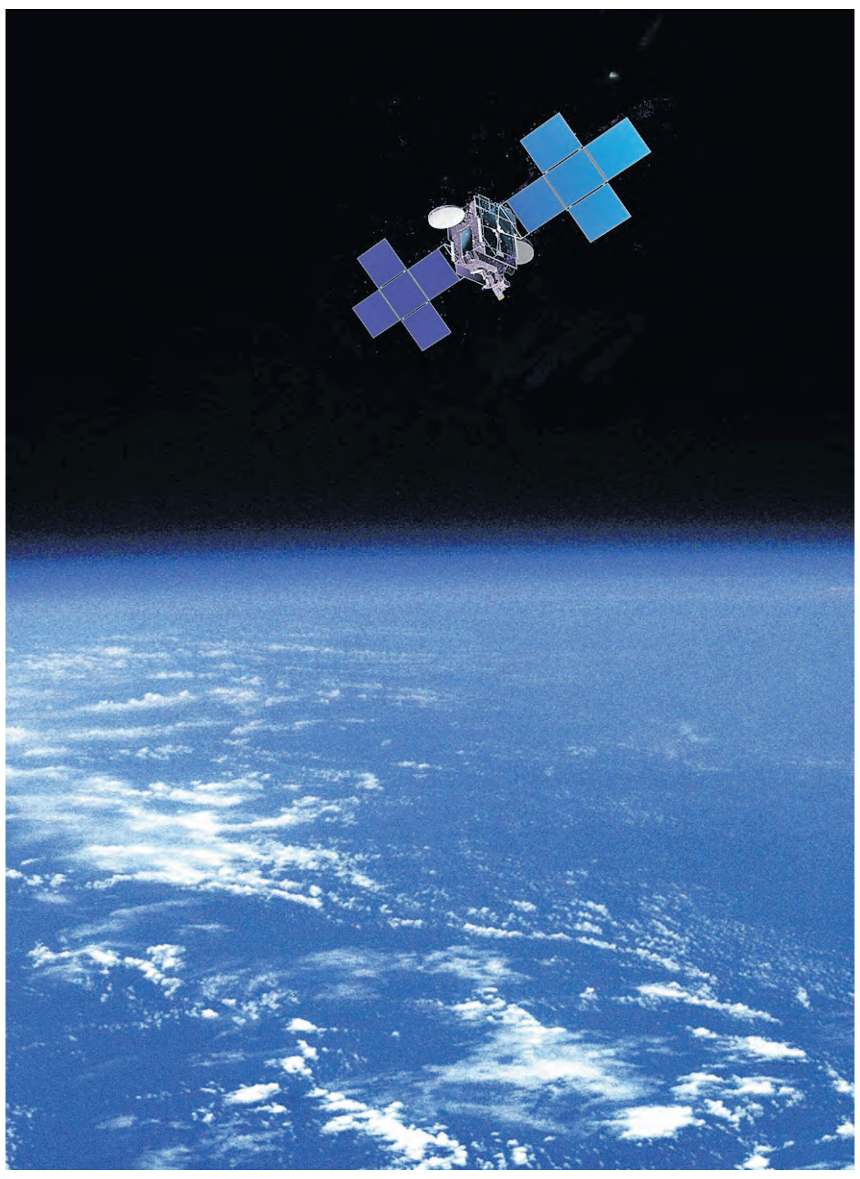
Atomic clocks on global positioning system (GPS) satellites allow the financial industry to co-ordinate trading across multiple time zones. Aircraft, ships, cars and military personnel use navigation satellites and broadband internet can reach rural locations and moving objects such as trains. Telecommunications satellites provide audio and video connections. Earth observation satellites provide imagery used by the military and governments in early warning weather systems and to monitor the environment.

Given that satellites are computer-dependent, they are susceptible to cyber security attacks. Two components of the satellite infrastructure are vulnerable: the ground-based components and on-board computers.

Attackers may be individuals, organisations or hostile governments. Activity could be politically motivated (sabotage, espionage, censorship, propaganda, terrorism) or financially driven (industrial competition, theft of data or services). Hackers could simply be rogue thrill seekers or vandals.

One can imagine the consequences of significant interference with satellites. The outcome of a denial-of-service attack or manipulation of location data that affects airline navigation systems could be fatal.

Disrupting global transactions by targeting satellites could have serious economic outcomes, including the freezing of leading trading hubs.



Hacked: Tamil Tiger rebels used the satellite to broadcast propaganda (Composite image); Nasa/WENN

Satellites can and should be designed with security in mind

Jamming (intentionally blocking or interfering with a signal) can range from being an inconvenience to a grave concern, for example denying satellite information to military personnel.

Where jamming disrupts commercial services, companies risk reputational erosion and consumer backlash. This is a sector with estimated global revenue of $195.2bn in 2013, according to the Satellite Industry Association.

Hackers can potentially commandeer a satellite to distribute their content or to manoeuvre the hardware in a way that disables it — effectively turning it into a piece of space junk. (The latter event has yet to occur, but hackers did take control of a Nasa Terra Earth Observation satellite in 2008.)

Are hacking and jamming scenarios a realistic concern? Experience and recent research suggests that the risk is relatively high. The box above lists only a selection of known incidents.

A report by IOActive, a security consultancy, in 2014, found that vulnerabilities remain across many services, but that the satellite industry has been reluctant to respond.

This is potentially a costly oversight: the satellite industry should be thinking about what countermeasures can be taken.

Encryption, whereby information is encoded and ground stations and satellites must "recognise" each other, is now used mainly for government and military satellites, but it could be applied more widely.

Industry resistance is partly explained by the cost of operation and impact on performance, in that it slows down processing.

Satellites can and should be designed with security in mind. As well as the obvious, such as including the latest anti-jamming technology, satellites should be dynamic and changeable once in orbit. Benefits of such "future-proof" spacecraft include the ability to update software remotely and to impose changes intentionally to make a satellite a "moving target"for would-be hackers.

Protocols must be in place, should compromises occur. Fast identification is crucial, followed by the isolation of the effects and plans to mitigate impact. Secondary actions include identifying the perpetrator (if possible) and implementing proportional countermeasures.

As ever, people are the weakest link, and vetting, training and monitoring of staff by satellite organisations may go some way to preventing intentional and negligent lapses.

The goals for satellite security are much the same as for other sectors: confidentiality, integrity, availability and continuity of services. Satellites are vital to our daily functioning and an energetic approach to security issues is necessary to ensure a stable future.

Dr Jill Stuart is an academic based at the London School of Economics and editor in chief of the journal Space Policy. www.space-policy.com

The many dangers from above

Ongoing Jamming
Governments, allegedly including Iran and China, obstruct satellite transmissions for censorship purposes.

2002 Hijack
The Falun Gong spiritual group hacked the Sino Satellite, causing severe interference with broadcasts.

2003-2004 Jamming
Commercial telecoms satellites leased by the US military during the Iraq war were jammed by the opposition.

2007 Hijack
An Intelsat satellite service was pirated by Sri Lankan rebel fighters to send radio and television broadcasts to other countries.

2008 Hijack
Nasa Terra Earth Observation satellite twice fell briefly under the control of unidentified hackers.

2008 Eavesdropping
Insurgents in Iraq intercepted live video feeds from military drones; the feed shows potential targets and was being relayed to a US controller.

2014 Hacking
Hackers in China allegedly accessed US weather satellites. Data were briefly disrupted.

Password pitfalls prompt rise in additional layers of checks

Authentication

Interest grows in third-party 'identity brokers' to help businesses verify customers, reports *Paul Solman*

Setting up an online account is easy: your user name is usually your email address, you then choose a password, deal with a few security questions, perhaps respond to a verification email, and your account is ready to use.

Unfortunately, hackers are also finding accounts increasingly easy to penetrate. Stolen or misused credentials are the number one way to gain access to information, according to the annual Data Breach Investigations Report from Verizon, the US telecoms group.

The challenge for any organisation providing online services is to ensure that the person accessing the account is really who they say they are, without making it too difficult for bona fide customers to use the system. Some believe the answer may lie in using a trusted third party to verify a user's identity.

Two out of three security breaches exploit weak or stolen passwords, according to Verizon. "Somewhere in the region of 84 per cent of all of the [security] breaches that we investigated were the direct result of a weakened credential of some sort, whether it was a guessable password or a stolen password," says Tracy Hulver, the company's chief identity strategist.

Much of the problem is the sheer volume of passwords. With multiple accounts covering social media, retailing, email and other online services, many people have little time or inclination to choose and remember strong passwords.

Though password cracking software is becoming increasingly sophisticated, hackers' success seems to be more the result of user carelessness, says David Emm, principal security researcher at Kaspersky Lab, a cyber security group.

"We are not improving at dealing with human weaknesses," he says. "Hacking starts with tricking individuals, and business are still not doing enough to raise awareness among staff. Being secure is hard; being wide open is easy."

One way to strengthen a password is to supplement it with a second authentication method. Many banks give customers a keypad or token to generate an authentication code, while some are looking to biometric data such as fingerprints or voice recognition to provide additional security.

However, not all organisations that provide online accounts are able to implement extensive and secure authentication procedures.

"The [security check] process is very expensive," says Kristian Alsing, a cyber security director at Deloitte, the consultancy. "But trusted providers such as banks, credit-rating agencies or government agencies can provide high-quality information to verify identity."

Governments have been early adopters of such systems, and the needs of online authentication are also being met by verification specialists. The UK government has launched GOV.UK Verify, which allows users to access online services such as HM Revenue & Customs by using one of three approved organisations to authenticate their identities: the Post Office, credit information group Experian and Digidentity, a Netherlands-based digital identity company.

Digidentity, set up in 2008, also provides services for the Dutch national identification scheme, other European governments and organisations such as insurers.

Verification requirements vary. The UK, for example, specifies slightly different proofs of identity from the standard used by other European countries. But once clients have signed up to Digidentity's service, and their identities have been checked, Digidentity can be used to authenticate requests to log into online services.

Could this model of a trusted "identity broker" remove the need for users to have multiple passwords?

Dick Dekkers, Digidentity's director of business development, says there is increasing interest from the private sector. "The highest goal would be the ability to use the same service across borders to buy a book, do your taxes and buy insurance," he says.

Mr Alsing at Deloitte also says the sector has growth potential, although he believes the idea of an identity broker has some way to go before achieving wide public acceptance.

So, conventional passwords may be around for some time yet. "It's too early to retire passwords as a security measure," says Konrads Smelkovs, senior adviser in the cyber defence team at KPMG, the consultancy.

"Consumers are not as security-conscious as they should be, and the industry accepts this and recognises the need to follow another approach."

"It's hard to change people's mindset," says Mr Hulver at Verizon. "But I do I think that the user name/password combination will be superseded, with other methods being used [in addition] to make it more secure."

Star sting Celebrity data hackers pounce on login weaknesses

Celebrities are used to having their privacy invaded, but recent cyber attacks have taken intrusion to new levels, highlighting the risks of storing personal data on the cloud and the shortcomings of password protection.

In August 2014, hackers attacked Apple iCloud accounts of actresses Jennifer Lawrence (right) and Mary Winstead, leaking private photographs. The company said the accounts were compromised by attacks on user names, passwords and security questions, rather than by breaches of its systems. Then, in November, a large-scale attack on Sony Pictures gave hackers access to confidential documents concerning some of the film-maker's biggest names, including Angelina Jolie (left) and Cameron Diaz.

"Passwords rely on the user to set them and need to be strong, but users often don't bother," says Kristian Alsing, a cyber security director at consultancy Deloitte. "Password recovery systems can be easy to hack. They often involve your mother's maiden name, the brand of your first car and so on, which can be quite easy to find out." **PS**

Former spooks emerge from the shadows

Start-ups

Accelerators are helping to take experts' ideas to market, writes *Hannah Kuchler*

Connected: start-ups are finding support in San Francisco and beyond — Dreamstime

These days, cyber security entrepreneurs are more likely to be just out of the intelligence services than straight out of college.

Accelerators — organisations that help start-ups with advice and early stage funding — have sprung up specialising in cyber security, focusing not on hoodie-clad twentysomethings with smart ideas, but on experienced professionals with in-depth security knowledge.

Start-ups in this sector attracted $2.3bn of venture capital globally in 2014, up more than a third on the year before, according to data from PrivCo, a research company, as businesses hunt for an alternative to existing technologies to help defend against hackers.

But starting a cyber security company is not easy: instead of the downloads and users desired by consumer technology start-ups, they must win the trust of large corporate and government customers scared of a fast-changing threat.

Kevin Rowney, co-founder of Mod N Labs, a San Francisco Bay Area-based accelerator, is using his expertise as a serial security entrepreneur and former senior manager at Symantec to help others progress from an "idea on a napkin" to contracts, fundraising and building a team. Mod N Labs may take a stake in a company or just advise.

He says: "It is a turbulent time in information technology — a lot is changing fast and many big providers are doing a bad job at adapting. The result is big holes in the threat landscape . . . and a giant opportunity for start-ups in security."

He adds, though, that entrepreneurs need more help to sell new categories of security software to large multinational banks than they do to create apps for takeaway deliveries, for example.

Rick Gordon, managing partner at MACH37, a Virginia-based cyber security accelerator launched 18 months ago, runs a 90-day programme that helps technically focused founders learn the business skills needed to run a company.

"Our first-time entrepreneurs are often a bit older, with deep technical expertise," he says. To have that eureka moment, he says you have to have dealt with security issues and have been in the trenches grappling with vexing problems.

But, he adds, such people may not be as adept at communicating their value to seed investors or institutional venture capitalists, "so that is certainly one skill set we teach".

He points out that entrepreneurs need more than just a "compelling PowerPoint" presentation — they must have evidence of a real need among paying customers.

MACH37 provides a $50,000 investment for an 8 per cent stake in a nascent business, matching it again or going up to $100,000 at the seed round. Mr Gordon says he expects almost all the "exits" to be via mergers or acquisitions by strategic buyers, ranging from long established companies such as Symantec to newer businesses such as FireEye or Palo Alto Networks.

Roy Stephan, chief executive and founder of Pierce Global Threat Intelligence, a security start-up, was in the accelerator's first class. The company has received $1m from angel investors and is raising more.

Despite having been chief technology officer at start-ups in the 1990s, Mr Stephan felt he needed MACH37 to teach him the financial and legal aspects of running a business. He says the accelerator was a "springboard" that helped him develop what was a "very, very early, somewhat nebulous concept". He adds: "It probably would have taken me three years on my own"

In London, Alex van Someren, a venture capitalist, and Jonathan Luff, a former diplomat and adviser to the prime minister, are about to launch CyLon, which they hope will help entrepreneurs who want to commercialise intellectual property that came out of the intelligence services.

Commissioned by the Cabinet Office to write a report on how to generate revenue from such intellectual property, they concluded that accelerators and incubators would help with both the standard challenges encountered by start-ups and the unique hurdles faced by companies founded by former intelligence officers. So they started an accelerator themselves.

CyLon is forming partnerships with defence companies, government agencies and academia to mentor and sponsor start-ups, many of which have been founded by people with a background in government cyber security.

The first cohort includes a start-up using machine learning to study network activity, one building a highly secure home router, and another specialising in biometrics.

Mr van Someren says that in the past couple of years, those with cyber security skills and experience have found themselves in demand in the commercial world for the first time and need to learn how to sell to businesses as well as governments.

"The experience of the government agencies, both defence and intelligence, has a lot to offer," he says.

"This is somewhat of a novelty. There is plenty of innovation in academia and the commercial domain, but there are relatively few opportunities for significant publicly funded work to cross over into the commercial domain."

Danger within is top vulnerability

Insider threats

Organisations need to put protocols in place so that growing risk can be managed, writes *Ravi Mattu*

At a dinner for some of Norway's leading chief information officers last year, one story highlighted the challenge of managing an organisation's security.

A CIO told how his chief financial officer asked him if he could use Dropbox, the cloud-based service, to share company files. The CIO said no — but the CFO did it anyway.

Knowing smiles filled the room. It was a familiar tale and the type of incident that worries those responsible for data security. If senior managers break protocol, what hope is there for an organisation with thousands of employees?

So-called insider threat ranks as the leading cyber security concern for corporates. In a survey of more than 1,800 organisations in 60 countries by EY, the professional services firm, companies said "careless or unaware employees" were their number one vulnerability.

Revelations by Edward Snowden, a former US National Security Agency contractor, raised awareness

A number of shifts underpin the threat. The way people work has changed. Smartphones and cloud-based software allow remote access to sensitive information. Companies often use contractors for core tasks, so outsiders may have access to sensitive parts of systems.

The ubiquity of personal technology also means staff expect corporate devices and software to be as easy to use as those at home. And it is almost impossible to prevent anyone finding a workaround to use their technology of choice.

Scott Weber, a managing director at Stroz Friedberg, a US consultancy that specialises in cyber security, says the focusis no longer just on outsiders. "We are seeing more and more boards and audit committees asking . . . the CIO, the CSO [chief security officer], what are we doing about the inside threat?"

One reason for urgency, says Ryan LaSalle, managing director of cyber security at Accenture, the professional services firm, is the leaks by Edward Snowden, a contractor to the National Security Agency, about its practices.

Among the concerns are sabotage by a disgruntled employee and, according to Mr LaSalle, the chance that a departing staff member could take intellectual property to another company, a particular concern at software businesses.

Despite the risks, the EY report found that 37 per cent of organisations "have no real-time insight on cyber risks necessary to combat these threats".

Nearly two-thirds do not have "well defined identity and access management programmes", meaning most lack an effective system to monitor and control access to information.

What can organisations do? For a start, they need to adopt a multidisciplinary approach. This means setting up a number of data streams to monitor behaviour as a single incident may not reveal anything substantial.

With these in place, Mr LaSalle says, there are four steps to managing insider risk. First, limit exposure with bring-your-own-devices policies. "BYOD is great for driving productivity[but] you need to get the right balance and limit access to those who really need it."

Second, senior executives need to ensure that team leaders drive change through an organisation. Next, develop a benchmark of acceptable technology use. This makes it possible to identify what types of behaviour "stick out".

Finally, "game the system" by trying to wrongfoot the bad apples. Some of Mr LaSalle's clients, for example, deploy "decoy documents . . . stuff that looks juicy".

Mr Weber adds that tools are needed to interpret the data. A single event is usually not enough to certify a breach. By analysing several data points over time, patterns are more likely to emerge.

There must also be the understanding that threats evolve constantly and organisations must adapt quickly.

As Ken Allan, global cyber security leader at EY, says: "By putting the building blocks in place and ensuring that the programme is able to adapt to change, companies can start to get ahead of cyber crime, adding capabilities before they are needed and preparing for threats before they arise."

Contributors

Murad Ahmed
European Technology correspondent

Sam Jones
Defence and security editor

Hannah Kuchler
San Francisco correspondent

Ravi Mattu
Technology, media & telecoms news editor

Sarah Mishkin
Former San Francisco correspondent

John Reed
Jerusalem correspondent

Paul Solman, Jessica Twentyman
Freelance journalists

Jill Stuart
Academic and editor in chief of Space Policy

Jerry Andrews, Adam Jezard
Commissioning editors

Steven Bird
Designer

Andy Mears
Picture Editor

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

Editorial content in this report is produced by the FT. Our advertisers have no influence over or prior sight of articles.

Fresh resolve in war against an invisible enemy

Continued from page 1

The numerous agencies that are being created to swap tips will help, Mr Cole says, but they must focus on the hackers, not just signs of breaches. Mr Obama's proposals are encouraging, "but there's still a very long way to go."

In January the president proposed three strands of legislation, hoping Congress will help him make them law.

First, he wants to improve information sharing, to ensure potential targets co-operate to understand hackers, just as the criminals swap tips on underground forums. Organisations will be created to help companies share information with government by limiting their liability to privacy lawsuits if they do so. He also wants to create a centre to share data between government agencies and industry organisations for companies to swap knowledge with peers.

Second, the president wants a national data breach law that will force companies to tell customers quickly when their data have been stolen, replacing the patchwork of state laws that currently do this.

Third, he wants to increase penalties under the Computer Fraud and Abuse Act, in an effort to deter hackers within US borders. The executive order announced last week adds to these three, giving the US a way to use sanctions to impose penalties beyond its borders, but still only if the hackers are doing business with any US entities.

Cheri McGuire, head of global government affairs and cyber security policy at Symantec, is cautiously positive about the proposals. "I'm always optimistic when there is a focus, particularly at the beginning of a new Congress, on the issue of cyber security. But I'm also cautious in that we want to make sure any legislation that is eventually passed is smart legislation," she says.

Ms McGuire adds that in some areas, such as surveillance reform, the government is not being "aggressive enough" and that it is important not to see information sharing as a "silver bullet". She wonders whether giving liability protection to encourage companies to talk about breaches really would incentivise sharing. If not, companies may be given protection they do not deserve.

"The concern is that, if liability protection is too broad, then somehow organisations will feel they are not responsible for securing their own systems, for making sure they have the best security in place," she says.

For Jennifer Granick, director of civil liberties at the Stanford Center for Internet and Society and a specialist in cyber law, the problem is broader. She questions the government's whole approach to the cyber security problem.

"The diagnosis is wrong and the remedy doesn't fit the diagnosis," she says. "Sony Pictures gets hacked [allegedly] by North Korea, so we increase the penalties in the Computer Fraud and Abuse Act. North Korea couldn't care less what the penalties are. It is not getting prosecuted."

Ms Granick worries that information sharing will damage individuals' privacy as data on internet activity could potentially be used by other areas of government. On the data breach notification, she sees the proposed Federal statute as "less protective" than existing state laws, as most US companies have to comply with the strictest state law, that in California.

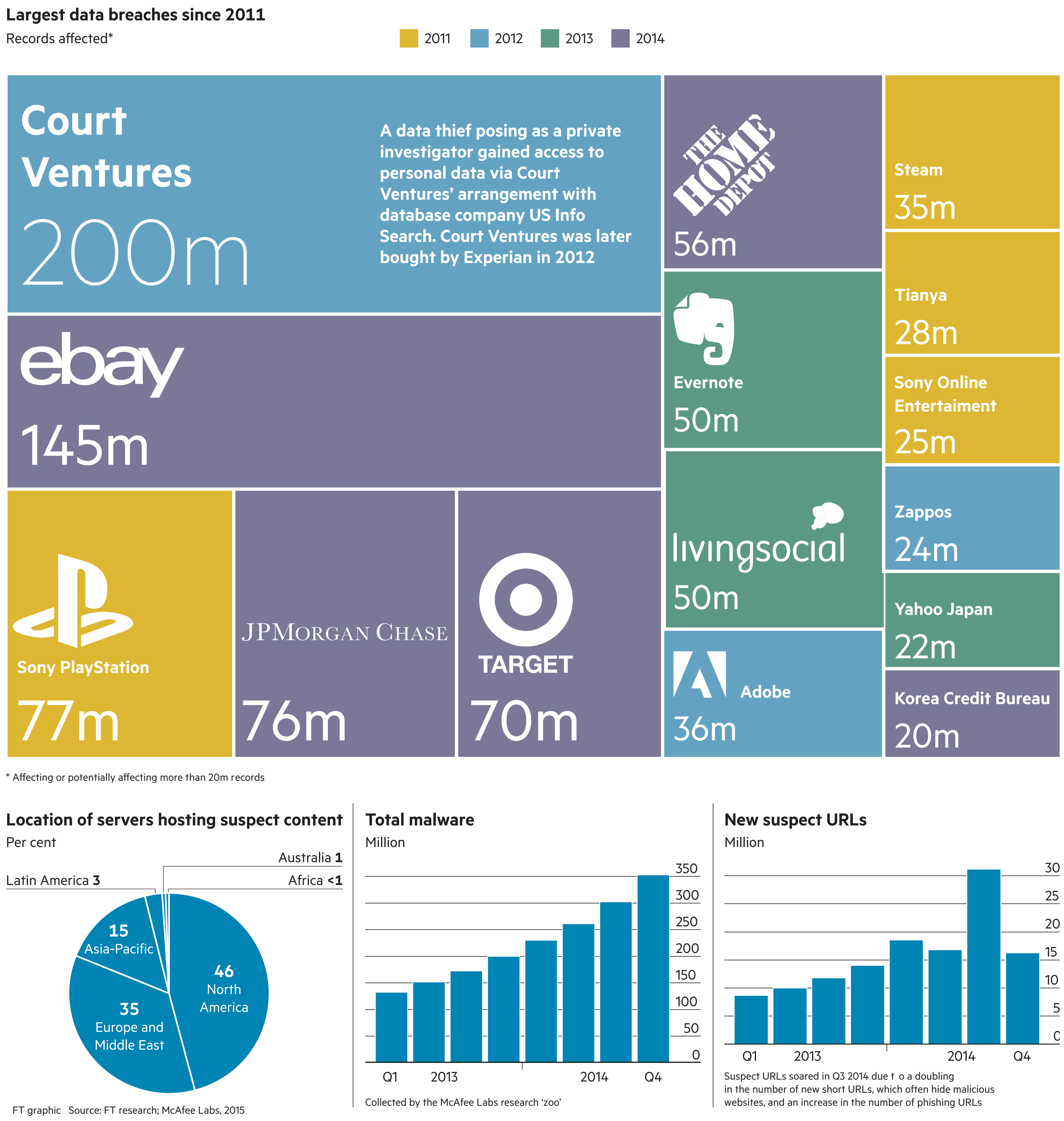
Ms Granick is concerned that increasingly hefty penalties could be used against security researchers, who probe vulnerabilities in systems to discover ways to fix them.

> 'North Korea couldn't care what the penalties are. It is not getting prosecuted'

Instead of piecemeal regulation, she suggests cyber security should be looked at in the same way as one would a public health issue. Companies should be pushed to have a basic level of security — for example, encrypting data and updating software — that would help stop less sophisticated attackers who are rife in networks.

"I think we're in a phase where looking at this as a criminal problem is not productive — we need a different framework, more like a national health model," she says. "It is a network we all depend on and it should be safe in the same way we keep the highways or electricity safe."

Cyber security threats



A data thief posing as a private investigator gained access to personal data via Court Ventures' arrangement with database company US Info Search. Court Ventures was later bought by Experian in 2012

* Affecting or potentially affecting more than 20m records

Collected by the McAfee Labs research 'zoo'

Suspect URLs soared in Q3 2014 due t o a doubling in the number of new short URLs, which often hide malicious websites, and an increase in the number of phishing URLs

FT graphic Source: FT research; McAfee Labs, 2015

Organisations faced with a battle on many fronts

Israel Technologies tackle increasingly sophisticated threats, says *John Reed*

At the Cybertech conference in Tel Aviv in late March, visitors could observe — alongside the cyber security industry's latest products and gadgets — the symbiosis between Israel's high-tech military, its government and its start-up sector.

Executives and fund managers sat alongside uniformed army officers in the plenary hall, or wandered the conference's Start-Up Pavilion to talk to entrepreneurs. Israel's National Cyber Bureau, part of Prime Minister Benjamin Netanyahu's office, led journalists — many from Asia — on a tour of exhibitors ranging from big incumbents, such as IBM, Elbit and Cisco, to new concerns vying for early-stage financing.

There was a panel discussion featuring veterans of Unit 8200, the elite military spying unit that was a pioneer in big data — sifting through masses of material to identify trends — and many of whose graduates enter high-tech businesses.

The biggest booth promoted the "CyberSpark" initiative in Beer Sheva. Cyber companies cluster around the city's university and tech park, and by 2020 two Israel Defence Forces military bases — including new headquarters for Unit 8200 — will be built nearby.

"You buy Swiss watches from Switzerland and information security from Israel," says Udi Mokady, chief executive of CyberArk, which listed its shares on Nasdaq in September in Israeli cyber's biggest public flotation of 2014.

"People know there is a lot of innovation in this space, and good engineering talent to wrap it into stable products that will not destroy what an enterprise is trying to do."

Israel, whose state bodies and companies are prime targets for hackers, built its cyber-related offensive, defensive and snooping functions as a product of its long regional conflict — "turning lemons into lemonade", as Mr Mokady puts it.

Now its moment to cash in on this expertise has come.

Last year's high-profile hacks at Sony, JPMorgan and Target brought home to global businesses an evolving and increasingly sophisticated cyber threat.

Companies' strategies are widening from a focus on malware and hacks from outside to a broader approach where they have to assume they can be targeted from within, and must be defensive on multiple fronts.

"There is no balance between attackers and defenders in the area of cyber," says Eviatar Matania, head of Israel's National Cyber Bureau. "We need to develop and produce technologies that enable us to balance this equation. Otherwise there is a real threat to western civilisation, to the economy, and to society as we know it."

The warning from Israel's top cyber-official might be interpreted as self-serving, given Israeli companies' increasing profits in the field. According to Mr Matania's office, Israel's annual exports in the sector exceed $3bn, and the country claims 10 per cent of the world's investments in cyber security.

However, non-Israeli executives share this view. Kris Lovejoy, IBM's chief information security officer, describes the threat to companies as "a war".

"We can't build fences around our organisation and expect to keep bad guys out; it's a biological warfare metaphor we are fighting today," says Ms Lovejoy. "Everyone is infected — everyone — [and] the bad guys are in our organisation."

Israel's start-ups and established companies alike are developing products to deal with this advanced threat.

CyberArk specialises in what it calls privileged account security — a layer or "digital vault" inside organisations' existing networks that can prevent an attack by someone who has attained inside access.

"We break a critical part of the cyber attack chain," says Mr Mokady.

LightCyber, another company showing its wares in Tel Aviv, describes its stock in trade as "active breach protection". Its product uses advanced algorithms to sift through mountains of data from users and devices to pick out potential malicious behaviour.

"We assume networks can get breached and attackers can get in," says Giora Engel, the company's chief product officer. "With our product, it's possible to detect the breach from the very first day, before there is damage."

BioCatch, another Israeli concern, provides "behavioural biometrics" to banks, ecommerce companies and others. Its product can detect malware or robotic activity, and gather information on how a user interacts with a password request or uses a mouse, then advises a client whether to go ahead with a transaction.

As the number of daily appliances connected to the internet worldwide grows into the billions, companies are developing protection from hacks for the Internet of Things.

Argus Cyber Security, another Israeli start-up, is developing protection for cars against hacker attacks on their telematics, infotainment units or other devices that are vulnerable through internet or Bluetooth connections.

The company, with a staff of 20 cyber engineers — including veterans of Unit 8200 — is working with carmakers and other industry entities, and has representatives in Germany, Japan and the US, close to the industry's big players.

Tom Barav, the company's marketing director, says: "We want to help prevent massive cyber recalls that could cost car manufacturers huge amounts."

Kris Lovejoy, IBM chief information security officer