FT SPECIAL REPORT

Cyber Security

Wednesday March 16 2016

www.ft.com/reports | @ftreports

Investors cool on start-ups that promise silver bullets

Sentiment towards industry sours as backers look harder at what companies offer, says *Murad Ahmed*

Last year was a boom time for cyber security start-ups. Just take a look at the deals. In November, Tenable Security, a Maryland-based company that specialises in spotting vulnerability in company networks, raised $250m in one of the biggest funding rounds for a cyber group to date.

The transaction capped off a bumper 12 months in fundraisings across the sector, with US peers including Cloudflare, Tanium and Zcaler each raising $100m or more.

But as the calendar flipped over to 2016 the boom was coming to an end.

Some entrepreneurs reported that securing funding had become increasingly difficult. Mike DeCesare, head of ForeScout, an internet-of-things security company, told the Financial Times in January that his company had raised $76m. But he said he felt like "the guy in the movie that slides right under the [closing door] . . . it is a very precarious investment environment right now".

The reason seems to lie in the general downturn facing the technology industry as well as the attitude of investors towards the cyber defence sector. But why should this be when the number of high-profile hacks of major companies keeps growing?

Since 2014, JPMorgan Chase, an investment bank, TalkTalk, a telecoms provider, Target, a retailer, Anthem Healthcare and Fiat Chrysler, a carmaker, have had their cyber defences breached. Their corporate reputations suffered as a result.

In February last year, the co-chair of Sony Pictures, Amy Pascal, left her job following a high-profile breach that led to private and embarrassing staff emails being published on the web.

A few months later, in August, Noel Biderman, chief executive of Avid Life Media, the parent company of Ashley Madison, an adultery website, stepped down in a move described as being "in the best interest of the company".

His departure followed a data breach that exposed the personal data of millions of customers who may have been seeking extramarital affairs. Weeks of damaging news stories followed.

Such attacks put some in the cyber industry in bullish mood for its future prospects. Take Austin Berglas, an executive at K2 Intelligence, a corporate investigations company and a former FBI agent.

> Sometimes it takes a JPMorgan Chase or a Target to make people prepare for an attack

Mr Berglas, who led probes into the Silk Road website, which sold illegal drugs and firearms on the "dark web", says: "Sometimes it takes a JPMorgan Chase or a Target to make people realise that the only way you can help yourself is preparation as though it's going to happen."

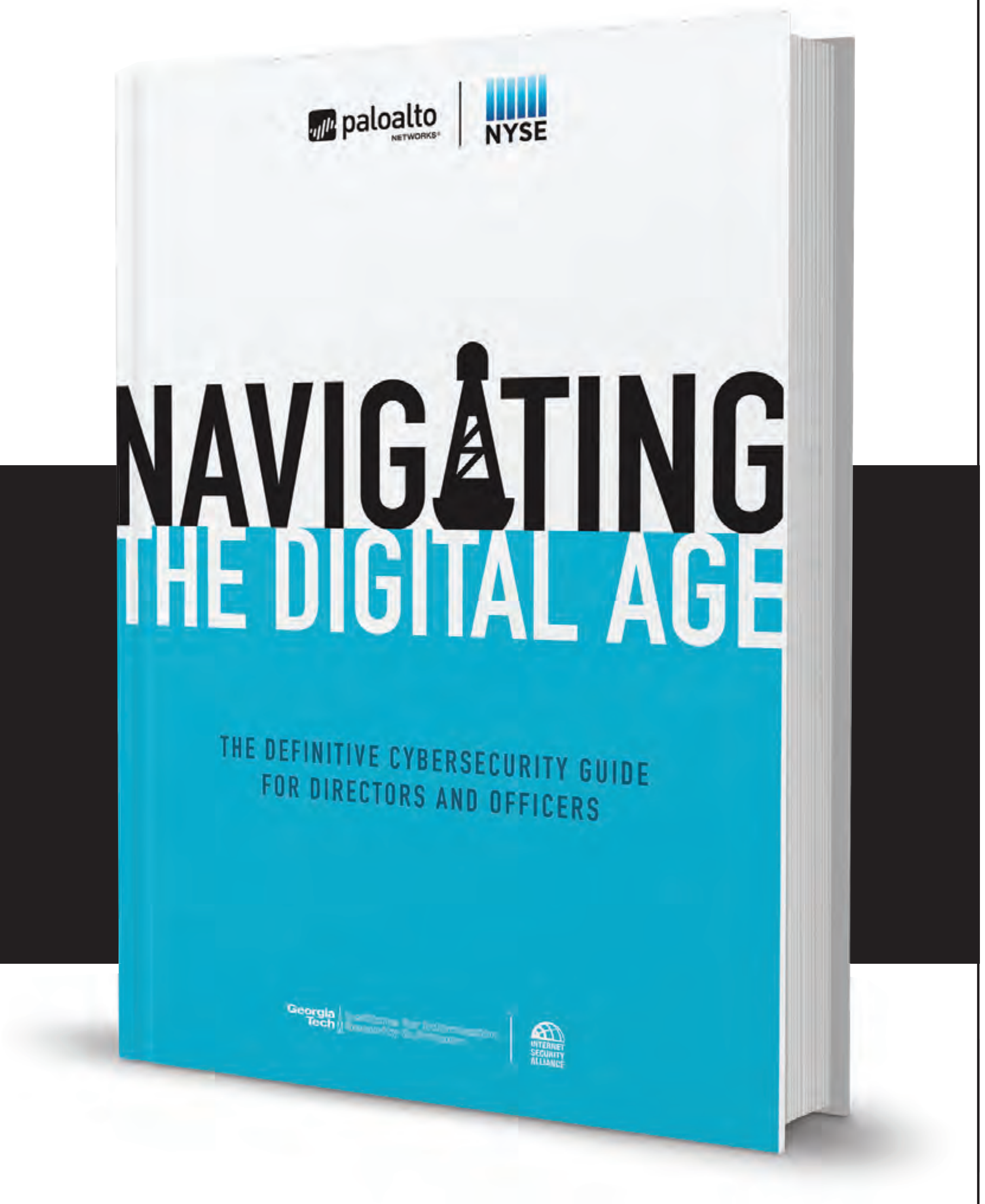
The cyber bulls' argument has some logic. Surely as companies and consumers wake up to the cyber threat they will want to spend more on defence?

Apparently not. Industry insiders give two reasons for the cooling in investor sentiment towards them.

The first affects all tech start-ups. A funding squeeze is hitting digital groups, with tech investors increasingly concerned about the soaring valuations enjoyed by start-ups, particularly in Silicon Valley.

Continued on page 2

Inside


paloalto NETWORKS
NYSE
NAVIGATING
THE DIGITAL AGE
THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS
Georgia Tech
INTERNET SECURITY ALLIANCE

Humble lightbulbs could become a form of attack

Internet of things The more objects connect, the greater the dangers, says *Stephen Pritchard*

If anyone in the technology industry believes the cyber security risk posed by the internet of things is exaggerated, then Daniel Miessler, a director at IOActive, a security company, is keen to put them straight.

IOActive has published a paper detailing how its researchers were able to take control of a sport utility vehicle without the investigators even touching the car.

The consequences of this type of attack could have lethal consequences, Mr Miessler says, but attacks on cars could be insignificant compared with risks to public transport, energy and utility networks and healthcare services.

Attacks could affect "infrastructure that is deeply ingrained [such as] power distribution, which is core to what we need as a civilisation", he adds.

Mr Miessler warns that assaults on critical infrastructure could even become common, both as a result of conventional warfare or cyber attacks.

His view is widely shared by those in the industry.

One reason for their concern is that older equipment in areas such as transport and utilities is being connected to networks — even the internet — for maintenance and monitoring.

Much of the existing equipment was designed for a pre-internet era and lacks the security and protection measures contained in a personal computer.

Cesare Garlati, chief security strategist at the PRPL Foundation, a non-profit open-source software group, says much of the hardware used in the internet of things, including older industrial control systems, were not designed to be "patched" or updated in the way a PC is. This leaves potential security flaws open to attack.

Industrial systems are not the only ones criminals might exploit. Many common connected consumer devices also face cyber hacking threats.

High voltage: everyday things may provide 'back doors' for criminals

"Things that are independently not that dangerous can pose a risk if they share information," says Mr Garlati.

"No one will be too concerned if you hack a car radio, but they will be if you can move on to attack things that are critical in the car."

He points out that in-car electronics and entertainment systems are more linked than ever.

Personal devices could also act as a "back door" to companies' computer systems, while the data they gather bring another set of security challenges and might even put a user's company at risk of attack.

Chris Underhill, head of information technology at consultants Cyber Security Partners, says that even something as seemingly simple as data gathered from a person's fitness band could help outsiders to launch a cyber attack against the user's company.

He says criminals may be able to see when security personnel are on breaks, or when few people are in the office, so an attack might go unnoticed.

Hackers could even take over thousands of devices, some as simple as a lightbulb, to disrupt a business or even a nation. Switching off one lightbulb could be a prank; plunging an office into darkness could disrupt a business; turning thousands of lights off and on at once could disrupt a whole power grid.

"People don't think what might happen if someone tries to do something malicious to a device," warns Justin Lowe, a security expert at PA Consulting Group. "An unimportant device might become important if connected to a critical system."

Despite these concerns, few observers believe the development of the internet of things will slow down because it has too many potential benefits.

"Humans want to be able to interact with machines in very efficient and expedient ways, and machines can benefit from interacting with machines in that way too," says Mr Miessler.

"It could be a toaster wants information from the refrigerator but it could be it wants information from the city's [power supply system] as well.

"There is a benefit from having them connected in a faster and more direct way," Mr Miessler adds. "But people are rushing towards that connectivity, and we have to deal with the security implications."

Ex-hackers are best placed to find chinks in your armour

Recruitment Executives tempted to hire those who learnt skills outside the law, says *Jessica Twentyman*

Reformed: Mustafa Al-Bassam outside Southwark Crown Court in 2013

Reuters/Luke MacGregor

The only British member of the LulzSec hacking gang to escape a prison sentence at the end of the trial at Southwark Crown Court in 2013 was Mustafa Al-Bassam, the youngest of those who had been in the dock.

The judge was said to have taken into account the fact Mr Al-Bassam was just 16 when the crimes were committed. He had pleaded guilty to charges of hacking and cyber attacks.

Mr Al-Bassam's co-conspirators Ryan Cleary, Jake Davis and Ryan Ackroyd received custodial sentences of 32, 24 and 30 months respectively.

However, for his role in LulzSec's "50 days of Lulz" campaign in 2011, the south Londoner was given a 20-month suspended sentence and an order to perform community service.

The group — which also had members in the US, Ireland and Portugal — launched cyber attacks against companies including Sony, News International and the CIA.

Nonetheless, the gang was publicly lambasted by Andrew Hadik, lawyer for the Crown Prosecution Service, for actions he called "cowardly and vindictive", and for causing harm that was "foreseeable, extensive and intended".

Three years on and Mr Al-Bassam is now an IT security adviser at online payment processing specialist Secure Trading, a role he intends to perform while completing his degree in computer science at King's College London.

"In this industry, there is always demand for people who have talent, regardless of your walk of life or background," he says.

Meanwhile, Kobus Paulsen, Secure Trading's chief executive, explains what may seem to be an unusual decision by saying: "When it comes to IT security, I can't think of anyone better placed to provide advice than an ex-hacker."

He compares it to recruiting a reformed burglar to protect a jewellery store: "Better than anyone, they will be able to find the chinks in your armour, and explain how they would go about breaching your defences, allowing you to fix and improve them."

Other business leaders may be open to adopting similar, poacher-turned-gamekeeper recruitment strategies, according to a 2014 survey of 300 senior IT and human resources professionals by KPMG, a professional services firm.

More than half of the respondents said they would consider using a hacker to add insider knowledge to their security teams, while a similar proportion said they would consider recruiting an expert, even if that person had a previous criminal record.

However, Johnathan Kuskos, manager at cyber company WhiteHat Security's Belfast-based threat research centre, does not believe this strategy is necessarily effective.

"Nobody should confuse a hacking conviction with technical skill or prowess," he warns. He adds that, while some former hackers may be good technically the flipside is that "the really excellent ones are probably not the ones who'll ever be on the job market" because they are too good to get caught.

Many companies prefer less tainted talent, says Rik Ferguson, global vice-president of security research at Trend Micro, another IT security company. "It's not that they couldn't hire convicted hackers, but rather that they have little interest in doing so because there's a rich pool of talent out there of skilled people without a criminal record."

He says there has been a steady rise in the number of IT professionals training as so-called "ethical hackers" on courses run by industry-accreditation bodies such as the EC-Council and the Sans Institute. These teach the same methods cyber criminals use but with the aim of identifying security weaknesses and patching them up, rather than using them for illegal purposes.

Mr Ferguson himself is a certified ethical hacker, having successfully completed the EC-Council programme in 2010. He says that participants are obliged to sign a document at the outset in which they promise to only use the skills they have learnt for legitimate purposes — a kind of Hippocratic oath for IT security professionals.

"If you're found to have misused the skills, then the sanction is the removal of your certification," he says.

A large proportion of convicted hackers are bored youngsters caught in the act of perpetrating "low-skill, high-volume" attacks, says Charlie McMurdie, a former Metropolitan Police detective superintendent who took part in the investigation into — and prosecution of — the LulzSec gang. She is now senior cyber crime adviser at PwC, a professional services firm.

'Nobody should confuse a hacking conviction with technical skill'

She says: "As an employer, you've got to consider the restrictions. If you employ that individual, what's your liability if they go back to their old ways? Can you guarantee oversight for their work? Are they even permitted to travel abroad to work with international clients? Should you disclose their background in conversations with clients?"

That last point is one that Mr Paulson at Secure Trading clearly considered when hiring Mr Al-Bassam. "We will never compromise our client relationships and will always be sensitive towards their wishes. Mustafa will not have access to client systems without their explicit approval," he says.

And, as Mr Ferguson at Trend Micro says, most people deserve a second chance. "You do the crime, you do the time and you get on with your life.

"There's a strong argument former hackers should be able to find employment in the market using the skills they have and, if they can't do that, then the temptation to return to illegal activities may be all the stronger, because there's no way for them to use their skills legitimately."

Greater speed and complexity help market abuse evolve

Fraud

Data provide easy pickings for would-be manipulators, reports *Emma Dunkley*

Market abuse is evolving. Instead of insider trading — company employees illegally making money with stolen confidential information — digital criminals are now trying to manipulate markets.

In the US, the Securities and Exchange Commission last year announced fraud charges against 32 defendants for taking part in a scheme to profit from stolen non-public information about corporate earnings.

Among those charged were two Ukrainian hackers accused of stealing data from newswire services and 30 people from around the world who apparently traded on it, allegedly generating more than $100m in illegal profits.

"Hacking is increasingly being used as a tool to get insider information. The reason is the growing digitisation of data," says Malcolm Marshall, a global leader of cyber security at KPMG.

Tracking down these increasingly sophisticated market manipulators is tough. Financial institutions are becoming more vulnerable and their defences — often located in outdated systems — are coming under strain.

Mr Marshall says that if hacking occurs in one country and trading in another, it is harder for law enforcers to catch offenders because of differences in regulations and legal jurisdictions.

Improvements in technology are to an extent being blamed for this evolution. As the mechanics of data storage improve, more information and data are being collected.

"Is this type of cyber attack going to increase? Absolutely," says Kris McConkey at PwC, a professional services firm. "Hackers are increasingly focusing more on aggregators of information, from payment processors to healthcare insurance providers . . . Attackers are getting smarter about where to focus their efforts and think hard about maximising their return on investment."

Roger Miles, an expert on behavioural risk at the Berkeley Research Group, says: "What we're doing unwittingly is concentrating risk, creating-low hanging fruit for thieves."

However, he says calling this "cyber risk" is a misnomer. "Cyber is just a conduit, all it has done is export old behaviour patterns into a new medium," says Mr Miles. "The issue is that people approach cyber crime as if it were a technology risk, when it's a people risk."

Dealing with cyber threats is now at the top of companies' agendas. A global study by consultancy firm Protiviti shows cyber security risk has become a key area of focus in 73 per cent of companies' audit plans. While cyber security and insider trading are global concerns, countries have different reporting requirements. Companies in the US, for example, are required to disclose attacks, perhaps creating the impression more occur there than elsewhere.

'People think of cyber crime as if it were a technology risk, when it's a people risk'

Indeed, a study by the Institute of Directors and Barclays, the British bank, reveals "widespread under-reporting" of cyber attacks in the UK. It suggests that companies have been keeping quiet even though half of attacks resulted in interruption of business operations.

Although many companies and industries that aggregate data are potential victims, financial services groups, from banks to stock exchanges, are the most targeted. "They have a rich concentration of financial assets and customer data, which makes them attractive," said Mark Weil, UK chief executive of global risk adviser Marsh.

A big threat for stock exchanges is a disruption attempt, such as foreign government launching an online attack that can bring operations to a standstill, known as a "denial of service". Efforts to fend off such onslaughts could reverse the shift towards faster markets, including high-frequency trading, which depends on computer algorithms and high-speed internet connections.

For banks, the main risks include the theft of earnings results and customer data, and denial of service attacks that bring down their systems.

Banks are starting to develop surveillance detection systems to monitor communication flows internally and how individuals interact with people externally, Mr McConkey at PwC says. This is to see what information is being passed on and check whether any trading is undertaken as a result.

Yet while companies are attempting to bolster their defences, they will never be completely immune from attacks.

"With the growing sophistication of attackers, some will get through the defences. It's then an issue of minimising the damage that can be done, such as by encrypting data," said Mr Weil.

Communications are crucial, he adds, "especially in banks, where customers' confidence is key — there need to be appropriate levels of reassurance, and rapid restoration of service".

Investors cool on start-ups that promise silver bullets

Continued from page 1

According to figures from CB Insights, a research group, in a study published jointly with KPMG, a professional services firm, venture capital firms globally made $27.2bn of investments in start-ups in the fourth quarter of 2015, a fall of almost 30 per cent compared with the previous quarter.

In the US, venture funding fell to $13.8bn in the last quarter of 2015, down from $20.2bn in the third quarter. There were similar falls in Asia and Europe.

The second problem is more specific to cyber security outfits.

Investors in the sector, such as Mike Chalfen, a partner at London-based Mosaic Ventures, says that after years of bluster a more discerning eye is being cast over the efforts of cyber security groups.

A large number of fledgling companies are joining a crowded market offering "point solutions" that focus on one problem, such as firewalls and antivirus products.

Instead, true value is to be found in "platform" groups that have a broader range of products and services.

One example of this is Palantir, an artificial intelligence company that specialises in spotting cyber threats and helps identify terrorist suspects for US intelligence services.

Palantir has raised $2.3bn in funds so far, including an announcement of $880m in December.

"The market, in general, is getting more discriminating," says Mr Chalfen. "It's not just investor sentiment is more negative, but there is greater discrimination between companies you like and companies you love. To some extent, there's a healthy recollection that security has always been a difficult area to invest in."

He adds that too many start-ups were overvalued and their products were overpriced.

Norman Fiore, general partner at Dawn Capital, a venture capital group that is a keen investor in cyber security start-ups, says: "I don't want to call it a bubble, but you did have valuations that ran away.

"You had lossmaking businesses growing fast but burning through lots of cash. There has been a move back to looking for companies with sound business models."

Marcin Kleczynski, founder of Malwarebytes, which protects consumers and companies from malicious software, says it has been difficult for investors to differentiate between security companies in a frantic market.

Cyber companies need to avoid hype and clearly explain they offer only part of a solution

He says: "There is a lot of noise in the security industry."

Generating revenues helps to attract investors, Mr Kleczynski adds. His company grew more than 120 per cent to reach an income of more than $100m in 2015, the sort of figures that in December convinced fund manager Fidelity to invest $50m.

It may be the case the cyber start-up sector is experiencing a useful correction, forcing investors to look more carefully at the inner workings of inexperienced companies before making projections of their future performance. But that shift may prove painful.

Mr Chalfen adds that the market is suffering from "silver bullet" syndrome. "There are usually multiple ways of solving a security problem. There is rarely one."

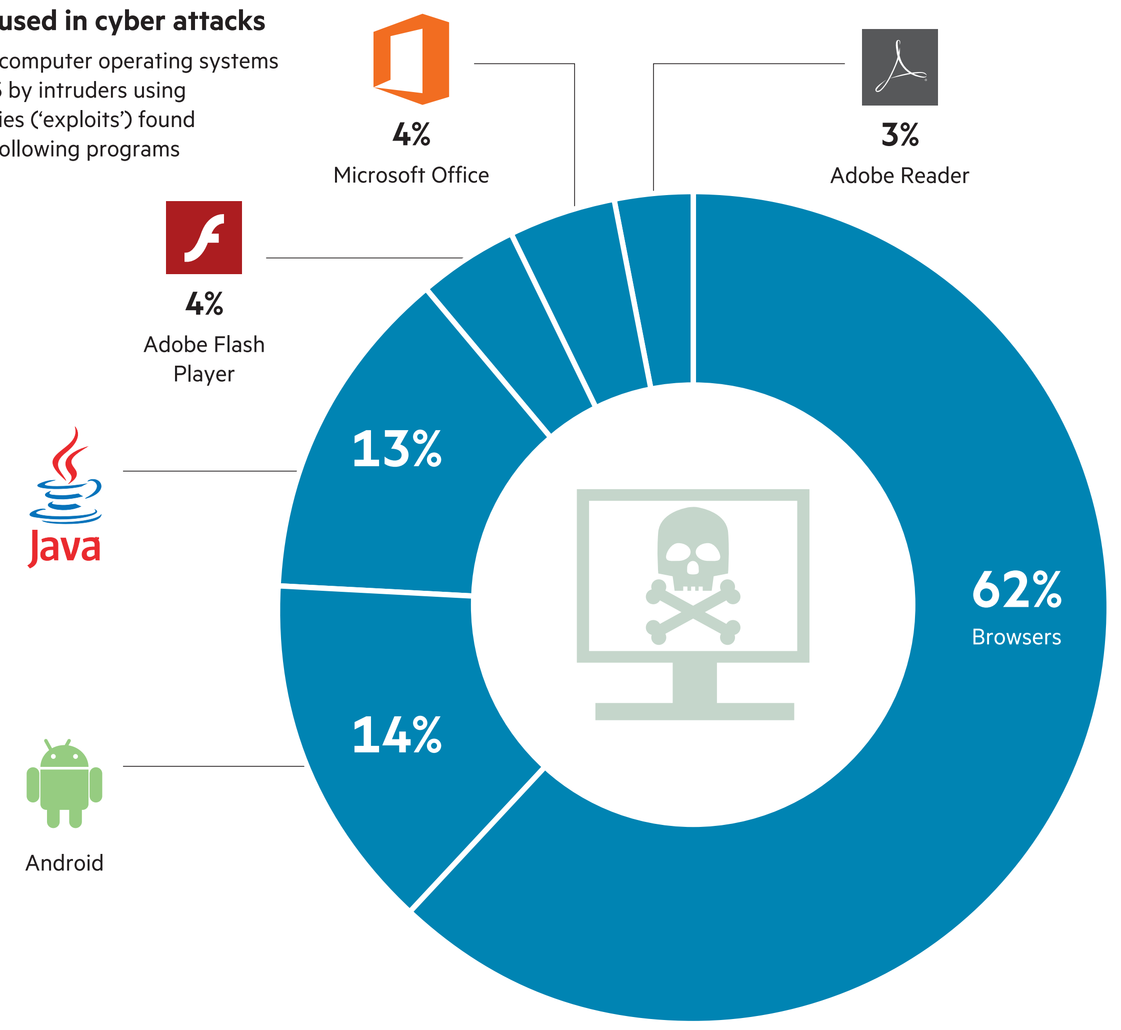
Mr Fiore says that cyber security companies need to avoid hype and explain clearly to their potential customers and investors that often they offer only part of a solution, not the whole answer.

Mr Fiore adds: "You layer and layer your technology so that, with a combination, [these layers] do more to provide protection."

2015: the year in cyber attacks

Exploits used in cyber attacks

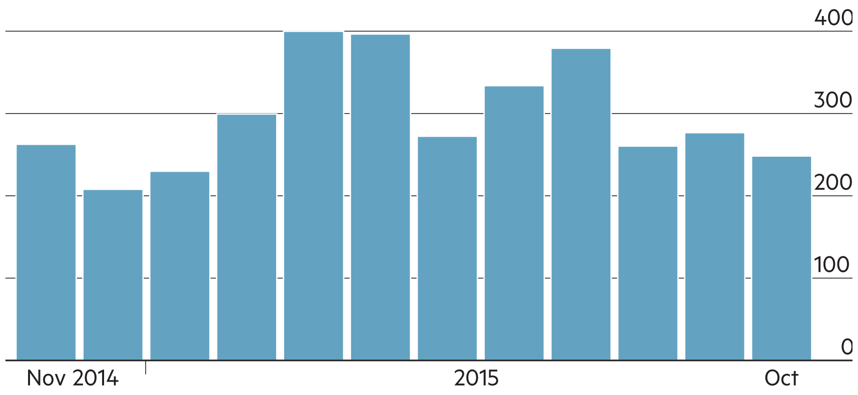
Attacks on computer operating systems during 2015 by intruders using vulnerabilities ('exploits') found within the following programs



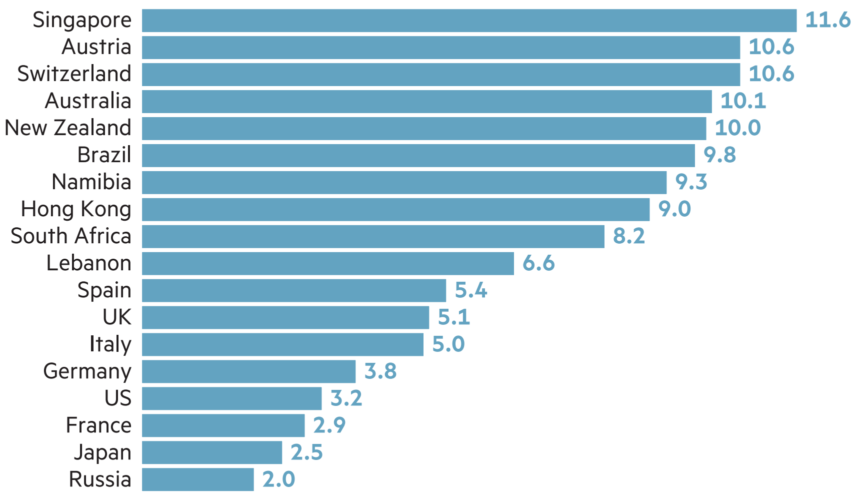
FT graphic Source: Kaspersky Lab, based on information from those of its 400,000 users who were willing to provide statistical data

Financial malware attacks

Blocked attempts to launch malware capable of stealing money via online banking on 1,966,324 computers



Banking malware attacks: countries by percentage of users targeted



Contributors

Murad Ahmed
European technology correspondent

Emma Dunkley
Retail banking correspondent

Maija Palmer
Digital editor, Special Reports

Stefan Stern
Visiting professor in management practice at Cass Business School, London

Jane Bird
Stephen Pritchard
Jessica Twentyman
Sarah Murray
Freelance technology writers

Adam Jezard
Commissioning editor

Steven Bird
Designer

Alan Knox
Picture editor

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

Advertisers have no influence over or prior sight of articles.
All FT Reports are available at: ft.com/reports

Rogue states play host to outlaw servers

Detection So-called bulletproof providers allow villains to conduct business, reports *Maija Palmer*

Criminals were already moving in to take advantage of the chaos in Syria when the civil war broke out. Even as the unrest increased and the country's relationship with the west became increasingly strained, a Russian-speaking group was setting up servers that could offer so-called "bulletproof" hosting services to online crooks.

Bulletproof hosting — so called because operators are beyond the reach of most law enforcers — enables cyber crime. It is the technological equivalent of a physical hide-out. Just as a gang needs a place to cache weapons and stolen goods, cyber criminals need internet-connected servers on which they can keep the malicious software they use for attacks, fake internet sites used for scams and the data they have stolen. Offering these hosting services to spammers, pornographers, data thieves and fake shopping sites has become an underworld business niche.

"We have seen the emergence of a full-service cyber crime model," says Bharat Mistry, cyber security consultant at Trend Micro, a security research company, which has published a report on bulletproof hosting.

He says: "It is easy for even a novice to get into this. You can rent the malware, get a support contract, and even a dashboard for monitoring an attack."

The cost of renting a dedicated bulletproof server is about $70 per month according to Trend Micro's research. Often the deal will include customer support services — such as a helpline number to call if things go wrong — as clients would have with a regular hosting arrangement. Alternatively, a server can be rented to mount a single attack for $5 a time.

Countries such as Syria, whose relations with the rest of the world have broken down, attract bulletproof hosts as it is hard for anyone to close their services down. IntelCrawler, a Los Angeles-based security start-up that specialises in profiling the cyber criminal underworld and malicious networks, discovered the Russian-language hosting business in Syria not long after the start of the civil war. Panama, Lebanon, Ukraine, Russia, and Iran are among the countries that Trend Micro highlights as being popular with bulletproof hosting businesses.

"International co-operation is non-existent with countries like Panama and Lebanon. And often there are no laws that allow you to take action," says James Aquilina, executive managing director at Stroz Friedberg, a computer forensics company. In many countries it is not, for example, illegal to send spam, or unsolicited email messages.

Bulletproof hosting is an often overlooked part of cyber crime, partly because these services are so difficult to track and shut down. There have been a few successes. In 2008 a hosting company called McColo stopped operating after two internet service providers cut off its access to the internet. Security companies estimated that the move resulted in global spam levels dropping by at least two-thirds. But such success stories are relatively rare.

Syria now: gangs find it easy to shelter in states where chaos reigns

Richard Cox, chief information officer at the Spamhaus Project, which tracks senders of spam, says his organisation is often able to trace malicious messages back to Russia and knows the identities of the criminals involved. Yet it is unable to act further. Cross-border co-operation with the Russian police has grown ever more difficult, he adds, following the UK inquiry into the murder of ex-KGB agent Alexander Litvinenko, which has heightened political tensions.

As well as choosing their geography carefully, bulletproof hosts use other techniques to make tracking difficult. They may, for example, hijack the servers of legitimate businesses, piggybacking on them to send out their malware. Sending out malicious messages at the same time as legitimate ones makes them harder to spot.

Bulletproof hosts often move operational bases quickly in order to escape detection. A 2014 study by Blue Coat Systems, a business assurance company, found that about 71 per cent of the websites around the world exist for less than 24 hours. A large portion of these "one-day wonders" were malicious sites, used to launch hacking attacks. By appearing and disappearing quickly they were able to escape detection by any filters and blacklists that companies use for protection.

"The rapid building up and tearing down of new and unknown sites destabilises many existing security controls," wrote Tim van der Horst, senior threat researcher for Blue Coat Systems, in a note about the findings.

"You are constantly chasing the flag, because it is always changing," says Laurance Dine, head of the Europe, Middle East and Africa forensics team at Verizon, a telecoms company. "An internet service company might receive complaints about malicious messages coming from a particular account, investigate and decide to terminate the account. Ten minutes later the same activities pop up under a new site."

Reputation fears drive ‘threat intelligence’ sector

Risk management

Websites mimicking real brands among new threats, reports *Jessica Twentyman*

How many of the people who follow you on social media sites really exist — and how many are lifelike avatars created by criminal hackers?

An investigation by IT security company Symantec unearthed dozens of fake profiles on professional networking site LinkedIn that had been created by scammers posing as recruitment consultants. The apparent aim of these fake profiles was to infiltrate business networks by making and exploiting connections with reputable executives.

Personal and professional lines blur on social media, where people are ready and willing to share information and curiosity persuades the unwary to click on web links of uncertain provenance.

“These are places where we build trust quickly with people who we believe share our opinions or enthusiasms — too quickly in many cases,” says Elad Ben-Meir, vice-president of marketing at Cyberint, a consultancy.

James Foster, chief executive of social media risk company Zerofox, says a common social media tactic is for fraudsters to assume the identity of someone’s colleague or business associate based on information gleaned from their online interactions.

The criminals may attempt to persuade their target to reveal system login credentials, divulge confidential company information or to download malware on to their company computers.

“Once the door’s been forced open in this way, then the potential for reputational damage is substantial,” says Mr Foster. “Just as most businesses put in place technology measures more than a decade ago to combat email phishing of their employees, I believe many will come around to the idea that a similar approach is needed to address social media risk.”

A study from IT security company Proofpoint, for example, says one in five clicks on malicious website links occur outside corporate email systems, mostly on social media and mobile apps.

Hackers are also using social media to manipulate customers. They pose behind fake profiles that represent legitimate brands or as a company’s customer service staff to lure people into divulging online banking passwords, provide personal details with the promise of free gifts or money-off coupons that never arrive.

The same Proofpoint study, for example, found that 40 per cent of Facebook accounts and 20 per cent of Twitter profiles claiming to represent Fortune 100 brands were unauthorised by those companies.

In 2015, airlines including JetBlue, Southwest Airlines and Virgin Atlantic had their brand identities hijacked by fake accounts on Facebook in order to dupe users into sharing personal details.

Customers had thought they were entering a lottery to win round-the-world, first-class tickets. While it is not known what the harvested data will be used for, it could well be sold on to other criminals.

In addition, fake web pages visited in order to enter these “competitions” may well install malware on users’ devices.

“Brands get tainted by this kind of ‘customer experience’, even though it’s clearly not the result of their own wrongdoing,” says Mr Foster. “In these situations, the burden of . . . making things right with the customer, typically falls to [companies].”

‘What most groups have in common is a lack of awareness of how widespread and serious the risks are’

Digital Shadows, a UK-based start-up, monitors social media sites, search engine results, online forums and the hard-to-reach, encrypted “dark web”, home to cyber space’s murky side.

James Chappell, the company’s founder, says: “We find spoof profiles, where hackers are impersonating employees and company executives and compromising brand integrity. We find sensitive documents all the time.

“Not every business faces the same risks, nor every industry,” he adds. “But what most organisations have in common is a lack of awareness of how widespread and serious the risks are.”

Where there is fear, there is an opportunity for security providers, as services and products that offer to provide protection from reputational threats will come at a cost.

Rick Holland, an analyst at technology market information provider Forrester Research, says concern about the unknown dangers is helping to drive what he calls the “cyber threat intelligence” sector.

Mr Holland adds he has already identified more than 20 companies that are attempting to grab a slice of this potentially lucrative market. It is likely more will join them.

CEO email scam is wake-up call for boards

COMMENT

Stefan Stern

Fake emails apparently sent by chief executives to senior employees asking for money transfers are estimated to have cost businesses as much as $2bn in the past two years, the FBI has said. There have been more than 12,000 corporate victims worldwide. Are you sure your business will not be the next to fall for the scam?

It is ironic that businesses can suffer from the malign entrepreneurialism of the cyber criminal. “The internet was built for connectivity and speed, not security and protection,” according to David Lawrence, founder of the Risk Assistance Network and Exchange (Rane).

“For criminals, rogue states and mischievous ‘actors’, the digital world has become the ‘promised land’ — low risk and high reward — offering borderless reach, assured anonymity and defenceless victims who are not allowed to fight back,” he wrote in an article for the Wharton business school at the University of Pennsylvania.

Cyber security is clearly a board-level concern, but the expertise needed to manage it may not always be present around the table. This is not something those who have built careers over the past 30 years have dealt with, after all.

More than half the 10,000 businesses questioned by PwC for last year’s “global state of information security” survey have now appointed chief information security officers. Meanwhile, the UK market appears to be a particularly attractive target for cyber criminals. According to PwC, about 55 per cent of businesses have been attacked over the past two years. Globally the average rate is 36 per cent.

Last year’s attack on TalkTalk, the UK telecoms company, was a prominent example of what businesses are facing.

This is an urgent issue, not just for maintaining business continuity and avoiding losses. Breaching the EU’s new “general data protection regulation”, which should come into effect in 2018, may result in personal as well as corporate fines.

Cyber security is “no longer a dark art but an everyday business practice that must pervade every level of the organisation”, according to Greg Day, chief security officer in Europe, Middle East and Africa for Palo Alto Networks, a cyber security company. It is not simply or solely a matter for a couple of clever people in the IT department, he says.

What can the board do to spread that level of cyber crime awareness? Mr Lawrence’s colleagues at Rane have identified some key actions that can lead to greater cyber security.

- Develop and practise “cyber hygiene”. Carry out background checks on personnel to reduce insider threats, and insist on robust passwords and multi-factor authentication. Employees have to be kept up to date about the latest email scams.
- Know your vendors well, and manage them carefully. Insist that their security standards are high.
- Protect your “crown jewels”. Identify, and separately protect, critical data and systems (such as customer data, intellectual property and market-sensitive information).
- Practise your incident response plan. This will involve working across departments and avoiding silo thinking. External technical, legal and crisis assistance, and public relations experts may be needed.
- Assess your levels of security with regular “penetration tests” that might reveal weaknesses.
- Develop a cyber threat monitoring and sharing team and make sure you have some cyber security insurance, if you can find anyone to price it appropriately, that is.

Business life must go on. Believe all the hype from security consultants and you might never turn on a device again

Boards must realise cyber risk is attracting shareholder attention. According to EY, the professional services firm, only 17 per cent of UK businesses report on the cyber risks they face and what they are doing about them. David Patt, analyst in corporate governance for Legal and General Investment Management, has called this a “huge gap in transparency”.

That is why boards must give this matter due attention and make sure it is being managed effectively.

But it is important, too, not to overreact. Believe all the hype from security consultants and you might never turn on a device again. Business life and transactions must go on. But today they have to be conducted with ever more care, and it is employees — the human software — who are perhaps most likely to succumb to workplace attacks.

Improved spelling helps criminals to target victims

Trends Hackers are hiring professional linguists in their efforts to trick the unwary, writes *Jane Bird*

Fraudulent emails used to be easy to spot. They were written by people who did not know their target victims and had a weak grasp of language.

“In the past, recipients would find such emails unconvincing because of poor spelling, grammar, punctuation and choice of words,” says Cameron Brown, an independent cyber defence adviser. But hackers are becoming more professional. Employing linguists to make their emails more plausible is just one example of this.

“Today’s cyber criminals,” he says, “are well organised, with their own premises and teams assigned to specific tasks. They are flexible, nimble operations that even bring in specialists for particular projects.” And they are recruiting computer science graduates by offering big salaries, he says.

Hackers are hard to trace as they use part of the internet called the “dark web”. This enables them to act anonymously and hide their tracks. However, Sian John, a security strategist at Symantec, a cyber security company, says online crooks “operate on a standard working week, continually refining malware [software designed to disrupt or damage a computer’s operations] and putting significant effort into disguising spam as legitimate email”.

One of the most dangerous threats over the past year has been the Dridex “trojan”, which targets bank customers. Trojans are named after the Trojan horse. They are found in links or attachments in seemingly friendly emails but attack your system when opened.

Dridex comes in an email with a Microsoft Office document attached. If opened, it triggers a malware download that tries to generate fraudulent transactions. Symantec believes millions of Dridex emails are sent each day.

Ms John adds that about 16 per cent of malware now knows when it arrives on so-called “virtual” computers, which security professionals use for tests. On these it lies dormant, only activating when it lands on a “real” computer.

There has also been a rise in attacks that combine two or more approaches. While security professionals are busy worrying about the first, the second can steal in unobserved.

John Shaw, a vice-president at UK-based Sophos, says one of the most effective new forms of attack is ransomware. This encrypts data then removes the keys that open it. Recovery is usually impossible without paying the gang that launched the attack.

Last October, the FBI told US companies they might not be able to recover data from criminals who had deployed tools such as CryptoLocker, CryptoWall and Reveton, unless they paid a ransom. Ransomware is often delivered by unskilled people who pay tech-savvy experts to supply their needs.

David Emm, principal security researcher at Kaspersky Lab, a cyber security provider, says such attacks are profitable for criminals. “They are growing dramatically and we think it’s likely that they will even outpace banking trojans as a way for cyber criminals to make money.”

Mail alert: an older generation of cyber con artists were let down by unconvincing emails
Getty

Criminals are even setting up false identities on social media networks to gather personal information about targets *(see story above)*. This can range from knowing what clubs people belong to, the holidays they have booked and online orders they have made.

Such information allows fraudsters to compose persuasive emails, says Don Smith, technology director for Dell SecureWorks. “You are much more likely to click on a ‘track my parcel’ email if you have ordered something.”

Instead of writing malware, cyber criminals often focus on gaining a foothold in a target organisation’s systems. They then hijack legitimate software and use it for fraudulent operations.

Hackers quickly change methods of approach if they think it will deliver better returns, says Dell’s Mr Smith. For example, they are switching focus from consumers to businesses when attempting to steal money from bank accounts. “A business is likely to take much longer than a consumer to notice when £50,000 is removed,” Mr Smith says.

There is a diverse online market for hacking products and services. Adwind, which has been used against more than 400,000 organisations globally, is a ready-to-use malware toolkit that can be bought by anyone.

Mr Emm expects to see more platforms hackers can subscribe to that will provide them with services, and forecasts a rise in the number of “cyber mercenaries” who sell attack expertise and provide access to high-profile victims.

Another worrying development is the planting of malicious software in computers during manufacture.

In the past year malware has been found pre-installed on some devices from Chinese companies, including Huawei, Xiaomi and Lenovo. Once installed it is almost impossible to remove.

Court rulings threaten to upset defences against data breach claims

Litigation

High-profile cases are likely to make it easier for consumers to sue data holders, says *Sarah Murray*

In February, a Los Angeles hospital paid a bitcoin ransom equivalent to about $17,000 to retrieve its medical records after hackers attacked its network.

While the records were soon restored, the attack raises the spectre of cyber criminals causing harm to consumers if a healthcare provider is, for example, unable to find out about a patient’s drug allergies in an emergency.

If these and other types of attacks increase, so could the risks of companies facing individual consumer litigation and class action law suits.

Until recently organisations could take comfort from the difficulties plaintiffs in the US faced in demonstrating they had suffered material injury caused by lost data.

In the 2013 case of Clapper v Amnesty International USA, Supreme Court justices ruled that legal action could not be brought against a government surveillance programme as the plaintiffs could not prove they were at immediate risk of injury. This ruling was applied to cases involving attacks on retailers, hotels and others.

“It’s difficult to show damage, particularly right away after a security breach,” says Matt Karlyn, co-chair of the technology industry team at New York-based law firm Foley & Lardner. “And sometimes the damage might not impact a consumer base or shareholders until much later.”

The Clapper decision has been used by “defendants on the receiving ends of these suits . . . to ask the court to dismiss the case, and many have been successful”, says Michael Whitener, a Washington-based partner at VLP Law Group.

But lawyers have still found ways to bring suits against companies whose data have been breached. They might claim, for example, that consumers have been forced to spend money on credit monitoring services.

Courts will become more creative about defining what an injury might be

“Because of the prevalence of data breaches and the desire of courts not to leave individuals without remedy when their data have been compromised, we’ll be seeing courts getting more creative about how they define what an actual injury or a pending injury might be,” says Mr Whitener.

In some cases, courts may not dismiss a case immediately but allow the plaintiffs to attempt to prove they have suffered. However, these cases tend not to lead to court decisions.

“You get into discovery [the pre-trial process during which the parties obtain evidence such as sworn statements and other documents] and lots of costs for both parties,” says Mr Whitener. “That’s where defendants are ready to settle rather than proceed.”

However, decisions from a number of high-profile cases are likely to make it easier for consumers to bring suits against companies in the event of a data breach or cyber intrusion.

For example, in July 2015, the Seventh US Circuit Court of Appeals, overturning a previous judgment, ruled that customers of Neiman Marcus could potentially sue the retailer because they were at substantial risk of identity theft or becoming victims of fraud as a result of a data breach two years previously.

Another case that increases the chances of consumers suing companies after cyber attacks is Vidal-Hall v Google. While the case concerns misuse of private information, not a security breach, it is significant because in March 2015 the English Court of Appeal found the plaintiffs could use EU data protection legislation to claim damages for distress from Google in the US without having to prove monetary loss.

“Until this case came along, you had to show financial loss,” says Marc Dautlich, partner at London law firm Pinsent Masons. “Now all you have to show is distress. That’s a game changer.”

Vidal-Hall v Google also illustrates the global nature of litigation over security breaches. The claimants, who are based in the UK, argued they should be granted permission to serve a claim brought in the English High Court against a defendant in the US, a procedure that is called “service out of the jurisdiction”.

Mr Karlyn says the uncertainty for companies about the possible outcome of legal action is likely to continue: “We’ve yet to get results that can give us an indication of where this is all going.”

He adds that this lack of legal precedents means that companies may not invest heavily in cyber security because the hazards and financial implications of class actions are unclear. “Companies are saying: ‘Is there really a risk I’m going to be subject to a class-action lawsuit?’ ”

And it is not always easy for companies to know how to best prepare for cyber incursions as the threat is evolving all the time, adds Mr Whitener.

“It’s an arms race with the hackers to stay one step ahead of them,” he says. “That’s a moving target.”