ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 September 2015 www.computerfraudandsecurity.com

Featured in this issue:

Securing small businesses – the weakest link in a supply chain?

The UK government has announced the investment of £1m into a new scheme to help SMEs boost their cyber-security, and has issued guidelines for small businesses.

But is this enough and should larger companies be spending money on helping to secure their smaller partners and suppliers? Tracey Caldwell discusses some of the risks and threats faced by the supply chain and provides industry commentary on the issues and recommendations arising.

Full story on page 5…

The security issues of the Internet of Things

The Internet of Things (IoT) was first envisaged in the last century, but interest has picked up in the past 15 years or so. And there are many potential benefits.

However, owing to the wide range of sectors involved and their impact on everyday life, the security issues can have serious consequences, causing damage, disruption to operations or, in some scenarios, even loss of life. Colin Tankard of Digital Pathways looks at how we might head off these problems.

Full story on page 11…

Big data – the future of cyber-security or its latest threat?

Big data allows organisations to detect anomalous behaviour in near real-time by consolidating data from numerous sources into one large database.

But adoption is still only at the very early stage and commercial options are limited, although a range of cloud-based services are expected to emerge over time. A key issue here is that big data expertise in either an information security or wider sense is still thin on the ground, which means that such systems need to be treated with caution, explains Cath Everett.

Full story on page 14…

US Internal Revenue Service admits to much bigger attack using stolen information

The US Internal Revenue Service (IRS) has revised the number of people affected by scammers using stolen data back in May.

The IRS was the target of a massive data-trawling attack in which criminals used personal data acquired from breaches of other organisations in an attempt to retrieve further information from the IRS systems. At the time, it was reported that around 100,000 people had their data illegally accessed via the Get Transcript service on IRS websites that allow taxpayers to retrieve past tax records. The Get Transcript service was subsequently

Continued on page 3…

Contents

Editorial Office: Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.computerfraudandsecurity.com

Publishing Director: Deborah Logan
Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Computer Fraud & Security includes 12 issues and online access for up to 5 users.
Prices:
€1385 for all European countries & Iran
US$1503 for all countries except Europe and Japan
¥184 200 for Japan
(Prices valid until 31 December 2015)
Subscriptions run for 12 months, from the date payment is received.
More information:
http://store.elsevier.com/product.jsp?isbn=13613723

12986
Digitally Produced by Mayfield Press (Oxford) Ltd

Editorial

One of things that makes information security such a difficult and complex task these days is the sheer variety of motivations for an attack. This makes deciding where to spend your limited security budget a tricky business.

Once upon a time, hacking was largely the province of spotty teenage boys looking to have fun and cause a little, seemingly harmless mayhem. At least, that's the myth. It was never quite like that, but the early days of connected computers were certainly a simpler era.

Today, we tend to talk mostly about cybercrime (usually involving organised gangs), state-backed espionage and hacktivism. That covers most of the malicious activity on the Internet, but not quite all, as a recent attack on Mumsnet showed.

The site, which acts primarily as an online community for women, came under a sustained Distributed Denial of Service (DDoS) attack. This form of attack is generally the tool of choice for blackmailers and hacktivists, but that doesn't seem to have been the case here.

The attacker, or attackers, also hijacked the accounts of a number of 'Mumsnetters' and used those accounts to post bogus messages on the site. The home page of the site was also redirected to a Twitter account using the handle @DadSecurity (that account has since been shut down). And the most egregious and vicious part of the onslaught was when site founder Justine Roberts and another Mumsnet user were 'swatted'. This is when someone places a call to the emergency services claiming that a crime is in progress at the target's home in the hope that an armed response unit will be sent to the address. This is precisely what happened to Roberts in the middle of the night recently.

Mumsnet has reacted responsibly. It has been open about what has happened, including the leaking of around 3,000 usernames and hashed passwords. The site forced a password reset on all users and put in place processes to insist that users choose strong passwords, even though the account hijacking was almost certainly achieved via phishing rather than the cracking of hashes in the user database.

There is a criminal investigation in progress. And we don't yet know who is responsible. But none of this fits into the general patterns. There appears to be no hope of financial gain nor any clear political motive.

The 'DadSecurity' handle does invite speculation. A divorced father who has lost a custody battle, perhaps? Or maybe it's just some rather pathetic man who hates women on principle. It seems clear that misogyny is the driving force.

And that is the scariest thought. One can see how a serious political position or the chance to make money might encourage someone to acquire the skills and resources to mount an attack of this ferocity. The idea that such damaging weapons are available to someone with no more than a twisted worldview should concern us.

Yes, people do resort to even more dangerous weapons sometimes – such as guns. So we shouldn't get this too out of proportion. What's significant here, though, is how easy it seems to be to mount this form of attack. What does this mean? Are the capabilities so easy to come by? DDoS tools are readily available, as we've seen from the NCA's arrest of six teenagers recently. And it doesn't take much to make a malicious phone call. The phishing, account take-overs and breaches would require a little more in the way of technical knowledge, but we live in an age where people are familiar with technology, so maybe these things are easier to obtain than we would like. Or is it a case that our defences are so terribly weak?

– Steve Mansfield-Devine

…Continued from front page
shut down. It's believed the attackers may have been intending to file fake tax returns for the 2016 filing period in order to receive refunds.

Now the IRS says that an additional 220,000 people had all or part of their tax records compromised by the attack. And investigators have found an additional 170,000 unsuccessful attempts to retrieve information. But there still seems some uncertainty in distinguishing between genuine and fake uses of the system.

"The IRS will begin mailing letters in the next few days to the taxpayers whose accounts may have been accessed," said the IRS in a statement. "Given the uncertainty in many of these cases – where a tax return was filed before the Get Transcript access occurred for example – the IRS notices will advise taxpayers that they can disregard the letter if they were actually the ones seeking a copy of their tax return information."

The agency is offering a free credit monitoring service to affected people, as well as the use of an Identity Protection PIN (IP PIN) – a six-digit number that can be used on tax returns as a form of authentication.

The IRS systems themselves have not been breached – but other organisations have not been so lucky.

In the UK, mobile phone retailer Carphone Warehouse has suffered a data breach affecting nearly 2.5 million customers, with as many as 90,000 of them also having had their payment card information leaked.

The attack happened on 5 Aug 2015, the firm said in its announcement three days later. The breach was a result of attacks on its websites OneStopPhoneShop.com, e2save.com and Mobiles.co.uk which provide services for customers of iD Mobile, TalkTalk Mobile and Talk Mobile. While the firm's response was fast, it was also somewhat disjointed. For example, customers of the Mobiles.co.uk site were contacted separately from others affected, and the message sent out by its managing director, Bobbie Bhogal, seemed to suggest that it was the customers' responsibility to take action. The email suggested that they: contact their bank or payment card issuer; check their accounts for suspicious activity; check their credit rating; and report any fraudulent activity on their accounts to Action Fraud.

Carphone Warehouse said – as is usual in such cases – that this was a "sophisticated" attack and that "additional security measures" had been put in place. No details of how the attack occurred were revealed, but the incident has been reported to the Information Commissioner's Office.

Travel booking firm Sabre said that its systems had come under attack, and some investigators are linking this to the breach of the US Government's Office of Personnel Management (OPM) – with the same, allegedly Chinese, group being behind both attacks. Sabre said it is investigating but, at the time of writing, did not know whether sensitive information had been compromised.

London health clinic, 56 Dean Street, accidentally revealed the email addresses of a large number of its patients. The clinic sent out a newsletter email to 780 patients who had signed up to its Option E service, which lets people make appointments and receive HIV test results by email. However, the email addresses of all the recipients were included in the To: header of the message – visible to everyone who got the email – instead of being placed in the Bcc: header. The clinic has sent out an apology and set up a helpline.

Travel firm Thomson also made an email error, sending out the home addresses, telephone numbers and flight dates of 458 customers in a mass email. It offered an apology but no compensation.

Finally, retailer WHSmith was also embarrassed when it found that any message sent via a response form on its magazine subscription service website – managed by I-subscribe – was being copied to all users registered on the site. The firm claimed that only 40 people had been affected.

Ransomware hiding in the dark

Organisations need to start blocking Tor traffic now or face an increasing risk from ransomware, concludes IBM in its latest X-Force report. Other forms of attack are also using the anonymising benefits of the technology.

According to the IBM X-Force 'Threat Intelligence Quarterly, 3Q 2015', the firm is seeing a large increase in ransomware attacks, and in the development of 'ransomware as a service'. Many of these attacks exploit the IP-masking capabilities of Tor to keep the cyber-criminals safe, both during the infection stage and the subsequent payment processes.

Other malicious activities that make use of Tor include SQL injection, vulnerability scanning and denial of service, says the report. Between 1 Jan and 10 May 2015, IBM registered 180,000 'malicious traffic events' in the US emanating from Tor nodes. The Netherlands were close behind with 150,000 events.

The fact that vulnerability scanning is in the list won't be a surprise to most security practitioners, who see scans on their network logs all the time. However, IBM says that it has detected what seems like a shift from more basic forms of cybercrime to what looks suspiciously like espionage. In part, this conclusion is promoted by a shift the nature of the targets, with financial organisations dropping down the list and information and communications organisations moving up, along with manufacturing firms.

"A likely explanation is that these attacks are not after money – they're attempts to steal intellectual property and/or spy on company operations", the report says. IBM's advice for dealing with this problem is to identify Tor nodes and block them at the firewall. The IBM report is available here: http://ibm.co/1hTORyd.

It's not only legitimate organisations that need to worry about Tor. Dark web market Agora – probably the biggest marketplace of illegal goods and services since the take-down of Silk Road – has temporarily suspended operations because of concerns over vulnerabilities in Tor technology.

The operators of the marketplace said: "We have recently been discovering suspicious activity around our servers which led us to believe that some of the attacks described in the research could be going on and we decided to move servers once

Continued on page 20…

In brief

NCA arrests six

The UK's National Crime Agency (NCA) has made six arrests connected with the use of the Lizard Stresser denial of service tool. The online tool, created by hacking group the Lizard Squad, allows people to pay to attack websites for up to eight hours at a time. The six teenagers arrested had used the tool to target organisations including, "a leading national newspaper, a school, gaming companies and a number of online retailers," said the NCA in a statement. The Lizard Stresser first appeared in December 2014, when it was used by the Lizard Squad to disrupt the Sony PlayStation and Microsoft Xbox gaming networks. It was shortly after set up as an online service, but was itself hacked in early January 2015 and disappeared from the net. In addition to the arrests, the NCA was planning to have a word with 50 other people whose details were registered on the site. Following the arrests, the NCA's website was taken offline for about an hour by a DDoS attack. The Lizard Squad tweeted an image carrying the legend 'Stressed out' and the NCA logo. The NCA described the attack as a "temporary inconvenience".

The image tweeted by the Lizard Squad following a DDoS attack on the UK National Crime Agency.

Frankenstein malware

Japanese banks and other financial institutions are being targeted by malware that appears to have been stitched together using pieces of malicious source code that have been leaked or made public over the past few years. Dubbed 'Shifu', after the Japanese word for thief, it appears to contain code from a number of other banking trojans, such as Shiz, Gozi, Zeus and Dridex. There are also string obfuscation and anti-research functions lifted from the Zeus banking trojan and processes that erase the System Restore point of an infected machine that are similar to 2009's Conficker worm. The malware has been deployed in attacks against 14 banks in Japan and electronic banking platforms in Europe, according to IBM Trusteer. There's more information here: http://ibm.co/1PLhfgs.

Securing the IoT

With concerns mounting around the security of the Internet of Things (IoT), a new collaborative initiative has been established to respond to them. The Internet of Things Security Foundation (IoTSF) has been formed to promote security best practice in IoT systems. It is vendor-neutral, international and collaborative, say the organisers, and already has the backing of over 30 organisations from global brands to academic institutions. John Moor, representing the IoTSF, commented: "The opportunity for IoT is staggering. There are a great many possibilities for businesses in all sectors including manufacturing, transport, health, home, consumer and public services. However, there are ever-real security challenges that accompany those opportunities. It is vital to the adoption of existing and new systems that security is addressed from the start, that it is fit for purpose and it can be managed over the life cycle of the system. Our intention is simple – drive excellence in IoT security. Given the nature of IoT systems, this can only be done by working internationally and with others. We will therefore be inviting organisations throughout the IoT ecosystem, who have a commitment to secure products and services, to join IoTSF. We also intend to work with colleagues in other IoT alliances and the standards bodies." For more details, go to: www.iotsecurityfoundation.org.

Attackers don't need malware

Dell SecureWorks' Counter Threat Unit (CTU) research team is warning organisations that not all attacks rely on malware. In nearly all of the intrusions in the past year responded to by the Dell SecureWorks' Incident Response Team, cyber-criminals used the target's own system credentials and legitimate software administration tools to move freely throughout the company's networks, infecting and collecting valuable data. Traditional security solutions that focus on a threat group's malware and infrastructure (such as command and control IP addresses and domain names) are of little use when the hackers don't employ malware in their operation, or use it so sparingly and for such a short time that it leaves few traces behind, said Dell. The CTU commented that organisations need to focus on threat actor behaviour and have their networks instrumented to determine if activity is suspicious. There's more information here: http://bit.ly/1NQTeqI.

Snooping via baby monitors

In spite of vulnerabilities in IP-based baby monitors having been highlighted a couple of years ago, many of the products on the market are still vulnerable to hacking, according to new research by Rapid7. The firm evaluated nine models from eight vendors and found a number of exploitable flaws. In three cases, the firm classed these as critical. The Philips In.Sight B120, iBaby M6 and Summer Infant Baby Zoom created live video streams accessible by anyone because they contained no authentication controls. Attackers could also enable remote access (eg, telnet) and change camera settings. Other vulnerabilities found in the sampled products included the ability of an attacker to potentially gain access to every recorded clip for every registered camera across the entire service, and to add an email address of their choice to every single camera. There's more information available here: www.rapid7.com/iotsec.

NIST drafts guide to improve security

The US National Cyber Security Centre of Excellence (NCCoE) is requesting comments on a draft guide to help energy companies better control who has access to their networked resources, including buildings, equipment, information technology and industrial control systems. The centre, part of the US Commerce Department's National Institute of Standards and Technology (NIST), works with IT developers and providers to help businesses reduce their cyber risk. The US Department of Homeland Security reported that 5% of the cyber-security incidents its Industrial Control Systems Cyber Emergency Response Team responded to in fiscal year 2014 were tied to weak authentication. Some 4% were tied to abuse of access authority. The guide, 'Identity and Access Management for Electric Utilities', could help energy companies reduce their risk by showing them how they can control access to facilities and devices from a single console. The guide can be found – and comments can be left – on the NCCoE website: https://nccoe.nist.gov/.

Leicester is UK theft capital

If you assumed that most thefts of electronic devices in the UK happen in London, you're in for a surprise. A series of freedom of information requests made by security firm ViaSat to regional police forces has shown that, while most thefts in general do, indeed, take place in the capital, when it comes to electronic devices you're more likely to have your device – with all its valuable and sensitive data – taken from you in Leicestershire or the West Midlands. While thefts of devices such as computers, smartphones and tablets accounted for 27% of thefts reported to the Metropolitan and City of London police forces, they formed 31% of thefts reported to West Midlands Police, and 51% of those in Leicestershire – compared to an average of 19% nationwide.

Securing small businesses – the weakest link in a supply chain?

Tracey Caldwell

Tracey Caldwell, freelance journalist

Small and micro businesses are often now the weakest link in a supply chain. The UK government, defining micro businesses as firms that employ 0-9 employees and small businesses as firms that have 10-49 employees, has announced the investment of £1m into a new grant scheme to help SMEs boost their cyber-security.[1] In addition, it has issued cyber-security guidelines for small businesses.[2] But is this enough and should larger companies be spending money on securing their smaller partners?

NTT Com Security's latest Global Threat Intelligence Report highlighted the need for organisations of all sizes to concentrate on getting the basics right.[3] Stuart Reed, senior director, global product marketing, says: "A staggering 76% of the vulnerabilities identified through the report had been known for two or more years. Nearly 10% were over 10 years old. An easy and practical way for small and micro businesses to help protect themselves is to make sure they regularly update their applications and operating systems with the latest patches and fixes available."

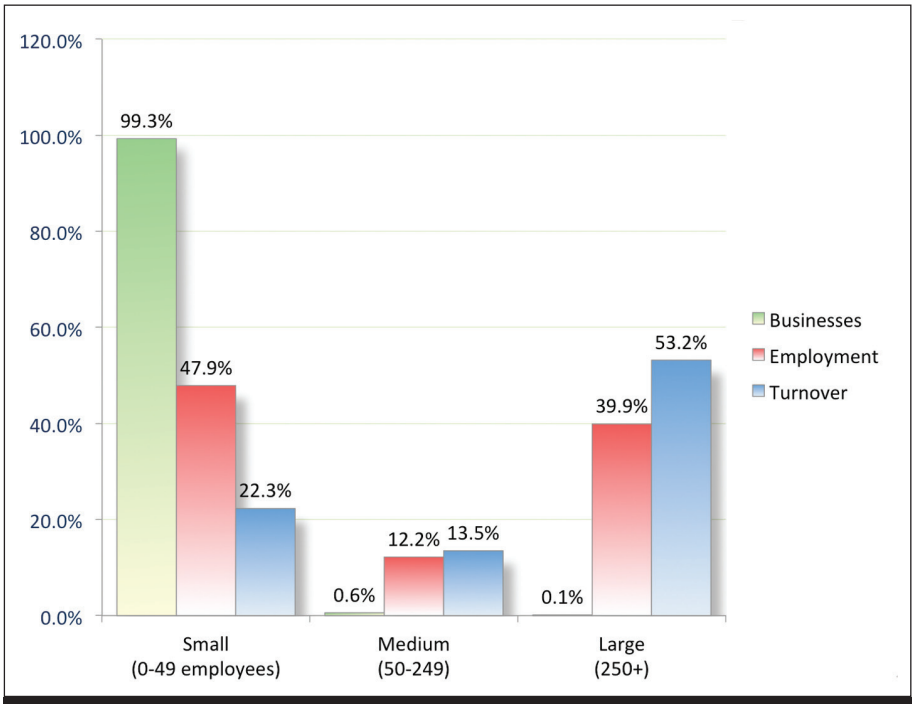
Stuart Reed, NTT Com Security: "An easy and practical way for small and micro businesses to help protect themselves is to make sure they regularly update their applications and operating systems."

The weakest link?

According to Scott Zoldi, FICO's vice president of analytic science: "Small businesses are particularly vulnerable to cyber-attacks – estimates are that more than 80% of attacks target small businesses as they are typically less well defended." FICO is well-known for the FICO Score, the standard measure of consumer credit risk in the US.

"Many times these businesses are resource constrained and focusing sparse resources on running the core business," he says. "The stakes are high though. When small businesses are breached nearly half go out of business within six months. Each business needs to take accountability for ensuring the basic cyber-security previsions are in place such as strong passwords, VPNs, employee education, virus protection, firewall configuration. Where there is a lack of knowledge, businesses can reach out to local cyber-security councils or assessment companies to help them with a plan to improve defences."

Oliver Pinson-Roxburgh, systems engineering manager at Trustwave,



Small businesses account for a significant proportion of the employment and companies in the UK. This graph shows the share of enterprises in the UK private sector in 2014. Source: 'Business Statistics', House of Commons Library.

points out that SMB and micro businesses tend to rely on e-commerce as their main payment acceptance channel and that represents a major threat to cyber-security.

"The stakes are high. When small businesses are breached nearly half go out of business within six months. Each business needs to take accountability for ensuring the basic cyber-security previsions are in place"

"With limited funds to invest in the development of applications, these organisations tend to use third parties that often put minimal to zero focus on security," he says. "According to our 2015 Trustwave Global Security Report, 98% of applications we tested in 2014 contained at least one security vulnerability. The maximum number of vulnerabilities our experts found in a single application was 747."

He adds: "Organisations will use common, cheap or free applications such as blog sites and shopping carts which are attractive targets for attackers – 30% of attacks we observed in 2014 were against WordPress. These systems are often connected to mission critical servers or contain customer data. The 2015 Trustwave Global Security Report also highlights that 49% of our 2014 forensic investigations involved the theft of PII [personally identifiable information] and cardholder data – rich pickings for attackers and easy to monetise."

Chris Sullivan, Courion: "Hackers will frequently seek out the access credentials of key employees."

Basic housekeeping

There are indications that micro businesses are not attending to basic low-cost security housekeeping. Chris Sullivan, general manager intelligence and analytics at Courion, believes that small businesses can underestimate the importance of how a business should organise and oversee employee user access, particularly privileged accounts, as hackers can easily manipulate these.

"Privileged accounts often provide broad administrator level access to resources and may have little oversight," he says. "Hackers will frequently seek out the access credentials of these key employees for use straightaway in compromising your system, or use them to further escalate privileges to gain access to more sensitive and valuable data."

Ross Brewer, vice president and managing director for international markets at LogRhythm, points out that the weak points in a small business are unlikely to differ hugely from a large business – the difference is in how they deal with the threat.

"While most organisations deploy some kind of anti-virus and a firewall, these tools are not enough to protect a network from today's advanced threats"

"It's all too easy for SMBs to persuade themselves that they aren't a target," he says. "The logic is fairly clear: why would a hacker go after a small business, when they could get far more from a larger organisation? While this theory may once have held up, today it simply isn't the case – everyone is a target and it's simply a case of when, not if, an attack takes place. While most organisations deploy some kind of anti-virus and a firewall, these tools are not enough to protect a network from today's advanced threats. Without far more robust tools in place, hackers are going to find it fairly simple to get in if they want to."

Charles Sweeney, Bloxx: "The main issue for both small and micro businesses is a simple lack of time and resources to dedicate to cyber-security."

Charles Sweeney, CEO of Bloxx says: "The main issue for both small and micro businesses is a simple lack of time and resources to dedicate to cyber-security. More often than not there is only a small estate of equipment for them to use to effectively secure themselves – sometimes just their own personal laptops. Resourcing issues can also expand to personnel, as many small businesses simply don't have the funds to employ dedicated IT staff to secure their network. A particular weak point in small and micro systems tends to be a lack of individual security clearance. Many will share log in details and have the entire business' data available to access."

Variety of compromises

Small and micro business may compromise cyber-security in a supply chain or similar business partnerships in a number of ways. The impact of a breach of security of small and micro business IT systems on larger organisations partnered with them or linked to them in any way ranges from data breaches, compliance issues and financial and reputational losses.

Margee Abrams, director, security services product marketing at Neustar, highlights the issue that, while most regulated industries undergo rigorous third party audits to ensure that they have implemented the appropriate security controls, "Their supply chain partners do not. Today, advanced adversaries attempt to gain a foothold in a target network, then move laterally to achieve their nefarious goals. A supply chain partner could provide this foothold through simple social engineering attempts. Or more sophisticated attacks can be achieved through dropping advanced malware through a supply chain channel via a phishing attack or USB drive."

"Today, advanced adversaries attempt to gain a foothold in a target network, then move laterally to achieve their nefarious goals. A supply chain partner could provide this foothold"

Increasingly, she believes, organisations will be required to vet their supply chain partners more thoroughly. "In fact, some government and military organisations around the world limit where manufactured items can be sourced from – software, microchips, etc – due to the risks associated with geo-hacktivism," she explains.

Reed at NTT Com points out that the supply chain invariably relies on trust between parties. If the smaller partner systems have been compromised, which subsequently results in a breach for the larger organisation, there is not just the cost of recovery, including enhanced security, PR management, brand damage for example, to consider for the larger company. "For the supplier, the trusted relationship is damaged – perhaps irreparably which, for the small and micro organisation, could mean that it will become more difficult to do business with the larger organisation or similar organisations in the future, losing out to competition," he says.

Margee Abrams, Neustar: "Sophisticated attacks can be achieved through dropping advanced malware through a supply chain channel."

"Security checks should be carried out on all partners to ensure they meet at least the company's minimum standards. What's more, every organisation, big or small, today should have the ability to identify unusual behaviour on its networks"

Reputational damage is a key issue for large organisations that are concerned about the security of small partners. "We've used the example before that when a zipper breaks on your jacket you don't blame the zipper maker, you blame the jacket maker," says Sullivan. "It's the same with your business partners, no matter how small they are, or how little impact they have on your overall business. When a small business has a breach, even if no data from the larger organisation is compromised, the breach still reflects on the latter's choices and can hurt the brand value of both businesses."

US retailer Target is a case in point. It suffered a data breach that resulted in the payment card information of 40 million customers being stolen, as well as personal information like email addresses and dates of birth of up to 110 million people. It's believed that the hackers gained entry by stealing log-in credentials from a contractor connected to Target's systems. Target settled a $10m lawsuit, with total losses resulting from the breach likely to be much higher.

"However, large organisations can't always make the smaller ones their scapegoat," says Brewer. "For a start, security checks should be carried out on all partners to ensure they meet at least the company's minimum standards. What's more, every organisation, big or small, today should have the ability to identify unusual behaviour on its networks. If a partner is accessing data they don't usually, perhaps at a strange time, or downloading vast swathes of information unnecessarily, it should be easily identifiable and, as a result, quickly stopped. Any business that allows others access to its systems, without this ability is asking for trouble."

The human factor

Dell SecureWorks has observed a number of cyber-attacks that target small and medium organisations, using them as a springboard to attack larger retail and financial services organisations further up the supplier chain. SMBs are seen as the weak link in security because their level of security investment and policies is far lower than the average large multinational. Critically, users in small and micro business are more likely to fall vic-

tim to phishing and social engineering attacks and act as an entry point into the larger organisation.

Hadi Hosn, security consulting managing principal at Dell SecureWorks, explains: "Businesses often forget the important role that employees play in preventing a security breach. Through no fault of their own, and mainly due to a lack of awareness, employees frequently open the virtual gates to attackers. Given that the end user is often the first to compromise security, businesses need to invest more in educating their employees and ensure that processes are simple and clearly understood to avoid a domino effect, which ripples through their partners and suppliers."

Enhancing user awareness of the threats is an easy win that will have a low impact on the IT budget in small businesses. There are other steps SMEs can take that would be a wise use of limited budget. "Determining what a company's most sensitive data is, keeping tabs on where it is stored, and minimising who needs to have access to it, is a key part of a solid IT security strategy," says Dell's Hosn. "There's no benefit to be gained from spending more on security than the information is worth. In creating one 'locked-down' area on a network, businesses will gain the benefit of a military-grade approach without incurring massive costs as only the most sensitive data needs to be behind a virtual barbed wire fence."

"Small and micro-businesses lack technical expertise, lack the revenue or margin to justify major infrastructure investments in security, and lack the staff to pay the appropriate amount of attention"

Small businesses need to focus on covering the basics, in Zoldi's view. "Many have issues such as running with default or weak passwords, employees that are not educated on phishing threats, not using VPNs, and a lack of understanding of PCI," he says. "Budget should be focused in two areas: one is getting a cyber-security review to ensure that the basics of the cyber defence are covered off so the business is not such an easy target; the second area is focusing on proper use of PCI standards, encryption, tokenisation – or better yet outsourcing this payment and customer details to a processor that can handle security of this sensitive data. One wants to ensure that if a breach occurs that the data that the cyber-criminals try to exfiltrate is encrypted and of no use."

Huggins recommends targeting a level of certification to reassure both the SME and its larger partners that basic cyber-security is in place. "Small and micro-businesses lack technical expertise, lack the revenue or margin to justify major infrastructure investments in security, and lack the numbers of staff to pay the appropriate amount of attention that the issue requires on an ongoing basis," he says. "Achieving Cyber Essentials Plus certification is a fantastic target for a small business. Outsourcing infrastructure and application security to cloud providers, for as much of their business as possible, is likely to make the most sense, as they can then focus their efforts on securing web browsers and users."

Government support

The UK government has put £1m into a grant scheme to help SMEs boost their cyber-security, alongside issuing cyber-security guidelines for small businesses. Hosn welcomes the move. "SMBs make up 99.3% of all private sector businesses in the UK, according to the Federation of Small Businesses," he says. "They represent a huge part of the UK economy and it's clear that this sector has already built or is currently investing in its digital footprint, but there is a very real cyber-security risk profile for these organisations."

He adds: "The new grant scheme will give SMBs access to security consulting and expert advice on securing their most sensitive information – the crown jewels, as it were. It's an initiative that SMBs should view in a positive light, considering that the cost of a large-scale incident could be considerably larger than the initial investment into the scheme. In addition, the guidance released by the government aligns with industry best practice, providing SMBs with a framework to implement cyber-security controls on their key assets."

"As long as businesses are given the right advice for protecting themselves from today's threats, not yesterday's, we have a real opportunity to ensure the UK's businesses are some of the most secure"

In Abrams' view, the UK government is wise to invest in the cyber-security of all of its citizens. "Hopefully, the output from this grant will be a clear, actionable framework for cyber-security best practices that small and micro businesses can reasonably implement," she says. "Very often, a right-sized 'templated' solution (such as common firewall rulesets) can help deter opportunistic attackers. Often, simple practices such as system hardening and patching are overlooked and result in serious data breaches that were preventable."

However, LogRhythm's Brewer believes the government guidelines are of limited value. "While it is great that the government is trying to push cyber-security further up the agenda, these guidelines only contain very basic information," he says. "Any organisation following it, and not doing anything else, will remain a risk. Many businesses are slowly waking up to the fact that reactive cyber-security measures just aren't going to cut it, and the government needs to be recommending far more robust procedures."

He adds: "The grants, on the other hand, are an excellent step forward. Many small businesses face budgetary challenges and cyber-security isn't high on the agenda of 'must-haves'. By giving them the additional resources to focus on this area, a lot of progress could be made. As long as businesses are given the right advice for protecting themselves from today's threats, not yesterday's, we have a real opportunity to ensure the UK's businesses are some of the most secure in the world."

Sweeney at Bloxx believes the £1m investment from the government into the SME cyber-security scheme won't stretch very far, unless it is properly managed and applied to the right areas. "This is what makes the guideline documents so useful; if they didn't exist, businesses would have to turn to third parties rather than themselves, where the £1m would dissipate into consultancy fees," he says. "It's also pleasing to see the guidelines emphasising the basics of good practice to businesses, offering a range of advice from passwords and spotting suspect emails to software and training. It's a valuable lesson for businesses of all sizes to remember: you can invest in the most hi-tech automotive security available, but the best way to stop your car from being stolen is still remembering to lock it."

Big supporting small

While government may have a part to play, should large organisations also do more to support small and micro partners to complete their cyber-security end-to-end? Phil Huggins, vice president of security science, at Stroz Friedberg, an investigations, intelligence and risk management company, says: "There is a strong argument that larger players in the supply chain should consider extending their information sharing and capability sharing to the smaller members of the chain, rather than punitively enforcing standards they cannot practically meet."

Abrams recommends: "Minimally, larger companies should require their supply chain partners to provide details about how they are securing shared devices and/or shared data between the organisations. Simple questions like the following are critical: do you have a corporate security policy? Have your employees been trained on the policy? How do you enforce security policies?"

She adds: "One example of a compromise attributed to a supply chain partner is the work of the extortion group 'Dragonfly'. Between 2011-2014, this group targeted the supply chain of Industrial Control Systems (ICS) in Europe and North America – replacing the partners' legitimate software with malware (ultimately downloaded by ICSs, including energy and pharmaceutical companies)." [4]

"Additional cyber-security controls and requirements for each partner could then be based on the criticality of the supplier to the overall large company strategy"

Sweeney, too, believes there is a responsibility for larger companies to look at their own supply chain and ask important questions about it. "When large companies go into business with a smaller supplier they will more often than not ask the same questions: how good is their quality and how financially secure and reliable is this business going to be?" he says. "In today's business world, the third question that should be added to that is: how robust is the online security of this supplier? And what would the implications be if they were breached onto my business?"

He adds: "Larger companies shouldn't have to invest in securing others and their links in the supply chain, but they do have the responsibility to check the security of smaller businesses and make sure there are no obvious warning signs that a supplier isn't secure. Most of the time companies will be asked to present their environmental policy, but it's high time that they also were asked for their cyber-security policy too."

In Hosn's view, large organisations have a role to play in securing the supply chain given the rise in the number of companies outsourcing their operations to smaller firms. "Large companies need to be clear on the cyber-security controls that their suppliers and small partners must implement," he says. "The security controls could be considered as the initial guidelines for a foundational cyber-security programme; additional cyber-security controls and requirements for each partner could then be based on the criticality of the supplier to the overall large company strategy. Large companies will also need to regularly assess the controls that SMBs have implemented to secure the large company's information, or to manage critical processes on behalf of the larger firm. This could be done through onsite security assessment visits, or self-assessment questionnaires that the SMB would need to complete."

Being compliant

Stuart Facey, VP EMEA at Bomgar, highlights the compliance angle. "For enterprise CISOs, it is important to remember where their responsibility lies," he says. "The recent changes in the Payment Card Industry Data Security Standards (PCI DSS) made it clear that responsibility over security always remains with the retailer, rather than with the outsourcing partner, for example.

"Small and micro SMEs might have a lower security capability, but their attack surface and visibility is also drastically smaller"

"There are two approaches that larger companies can take here: either they can reduce the amount of access that outside companies have to IT network assets and use internal skills or services instead. Alternatively, they can implement their

own privileged access management strategies to ensure that they are in charge of who accesses what IT assets and when, enabling their external suppliers to remain productive. Taking control of who can access their infrastructure can help to de-risk the situation for the large enterprise, keep their networks secure and limit the attack surface that can be targeted at both the large company and the SMB."

Orlando Scott-Cowley, cyber-security specialist at Mimecast, points out that information security standards also have something to say on this issue. "The updated ISO27001 standard enforces good vendor and partner management on organisations from an information security perspective, and ought to give us all a benchmark of best practice when it comes to securing our providers," he says. "For larger organisations, it is vital that they not only enforce a required standard of protection on their suppliers, but also help those suppliers reach that standard – for example, open network access to a supplier is not best practise. Giving the supplier a secure, encrypted portal which pre-checks devices before allowing access to the network is a much better idea. Larger organisations also need to check their suppliers regularly too; quite often backdoors and shortcuts get introduced over time, to make someone's job easier, and these are very often easy to detect and exploit."

Conclusion

A robust supply chain is critical for businesses of all sizes. "To preserve the integrity of the supply chain, many organisations may consider audits or assessments of partners to make sure they meet their defined security criteria. If small and micro business can demonstrate adherence in this regard, it not only shows best practice but may also drive completive advantage against others that have not placed the same rigour around security and risk management," says Reed at NTT Com.

Security as a service offers the same 'pay as you go' benefits as other cloud services and may offer SMEs an affordable solution. Thomas Owen, security manager of UK cloud-hosting provider Memset, says: "The financial barrier for entry into mature cyber-security controls, where an organisation can reliably detect and respond to complex attacks, is higher than almost any small or micro SME can afford. Security-as-a-service offerings and some of the more innovative small-scale IT outsourcing and hosting companies are helping to redress the balance, but without the budgets of a major bank or SI, a different paradigm is required."

Owen does point out, however that the metaphor of SMEs being the weakest link in the chain could be disingenuous. "Small and micro SMEs might have a lower security capability, but their attack surface and visibility is also drastically smaller. Risk being a function of impact and likelihood, a large corporation or outsourcer – classic aggregation of risk – is subject to a far higher level and rate of attack, one that they're not necessarily more likely to be able to respond to."

He concludes: "Small and micro SMEs can also punch well above their weight when compared to large, high-overhead, bloated established businesses where security and risk management are an integral part of their operation or USP. Finer margins, higher agility and a tighter organisational focus can all lead to an organisation that can leverage its resources with much higher efficiency and adapt to the changing risk landscape.'

About the author

Tracey Caldwell is a freelance business technology writer who writes regularly on security issues. She is editor of Biometric Technology Today*, also published by Elsevier.*

References

1. Rhodes, Chris. 'Business statistics'. Briefing paper, House of Commons Library, no.06152, 28 May 2015. Accessed Aug 2015. www.parliament.uk/briefing-papers/sn06152.pdf.
2. 'Small businesses: what you need to know about cyber-security'. HM Government. Accessed Aug 2015. www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf.
3. 'Global Threat Intelligence Report 2015'. NTT Com Security. (Registration required). Accessed Aug 2015 www.nttcomsecurity.com/en/services/managed-security-services/threat-intelligence/.
4. 'Cyber-security risks in the supply chain'. CERT-UK. Accessed Aug 2015. www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf.

Recommendations for small businesses

NTT Com Security's research resulted in the following recommendations for small businesses:

- Get the basics right – without the practical fundamentals, attacks don't need to be advanced to succeed.
- Define and test incident response – active incident response is critical to minimise the impact of security breaches, but must be aligned to, and cover, all aspects of your business objectives.
- People are the greatest threat – invest in staff awareness and training, highlighting the importance of collective responsibility.
- What you don't know can harm you – use threat intelligence to put risk in context for your business.

The security issues of the Internet of Things


Colin Tankard

Colin Tankard, Digital Pathways

The Internet of Things (IoT) was first envisaged in the last century, but interest has picked up in the past 15 years or so. It is a vision whereby potentially billions of 'things' – such as smart devices and sensors – are interconnected using machine-to-machine technology enabled by Internet or other IP-based connectivity.

A recent study by the McKinsey Global Institute estimates that the IoT will have a potential economic impact of $3.9tn-$11.1tn per year by 2025 across nine settings – homes, offices, factories, retail environments, worksites, human health, outside environments, cities and vehicles.[1] Estimates vary widely regarding how many IoT devices will be connected, but an often quoted statistic is from Cisco, which estimates that 50 billion objects and devices will be connected by 2020.

Potential benefits

There are many potential benefits from embracing the IoT. Verizon estimates that currently some 10% of organisations have adopted IoT extensively and that, by 2025, those that do so will be 10% more profitable than those that do not. They will be better empowered to innovate, disrupting both established players and new entrants, and will afford their customers better experiences, see accelerated growth and improved performance, and will be able to improve safety and reduce risk. For example, IoT will enable new ways to protect inventory, equipment and machinery, even in remote locations or over large areas.

According to a recent survey by the SANS Institute covering organisations of all sizes, 66% of respondents are either currently involved in or are planning to implement IoT applications involving consumer devices, such as smartphones, smartwatches and other wearables. Smart buildings systems are increasingly being implemented as operations management systems get connected to networks. The IoT holds much promise for the energy, utilities, medical devices and transport sectors, which will see the highest levels of adoption in the near term, according to SANS, as well as smart buildings.

Smart buildings

Smart buildings are those in which the various systems, such as lighting, heating, ventilation, air conditioning and security, are connected. In terms of security, connected alarms, sensors and tracking devices will make threat detection easier and remotely activated cameras and other networked security equipment will help to improve physical security. Other benefits are higher operational efficiency, more safety and comfort, and lower cost of operation as systems pass data freely back and forth.

"The IoT holds much promise for the energy, utilities, medical devices and transport sectors, which will see the highest levels of adoption in the near term"

The EU has identified further development of smart buildings as an imperative for achieving its goals of a proposed improvement in energy efficiency of 27%

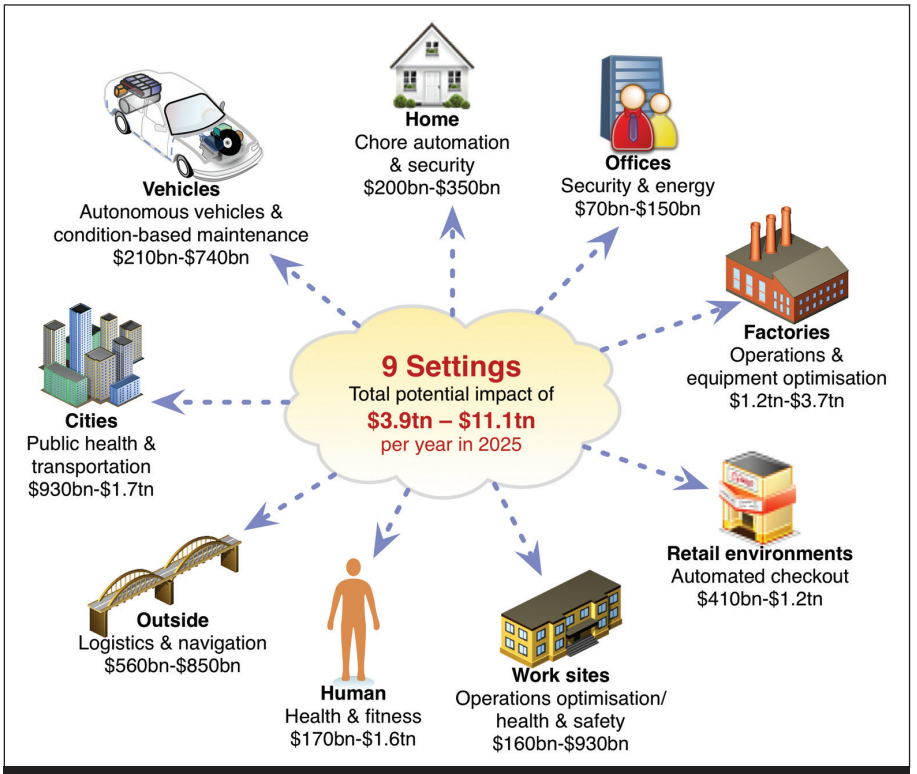


Figure 1: Nine settings identified by the McKinsey Global Institute and their global impact by 2025.

by 2020, potentially 30% by 2030, under the Energy Efficiency Directive set out in June 2015. It states that new buildings now use half of the energy that they did in the 1980s owing to the use of new, smart technologies.

The US is also focusing on this sector, aiming to increase energy efficiency in buildings as well as reduce energy costs. It passed the Smart Building Acceleration Act in May 2015, which it is hoped will be a catalyst for increasing the transition to smart building technology across the country, in both the public and private sectors.

Security issues

While the IoT holds much promise, many security issues have been uncovered. Owing to the wide range of sectors involved and their impact on everyday life, such security issues can have serious consequences, causing damage, disruption to operations or, in some scenarios, even loss of life. In a smart building – where systems ranging from HVAC (heating, ventilation and air conditioning), lighting and door access controls, to video surveillance and elevators, are all interconnected – a security threat that is exploited to disrupt power or lighting could cause loss of life if it were something like a hospital. In office buildings, a door access control that is hacked could provide an intruder with unauthorised access. Issues with IoT devices are far from hypothetical: one example of a threat is the Stuxnet worm, which has been seen to be able to disrupt industrial control systems, causing extensive damage.

"A different stance needs to be taken. Security needs to be built into products by design. It cannot be bolted on afterwards"

A range of security risks have been uncovered in the devices themselves that make up the IoT. OWASP has identified the top 10 such issues involved with IoT devices:[2]

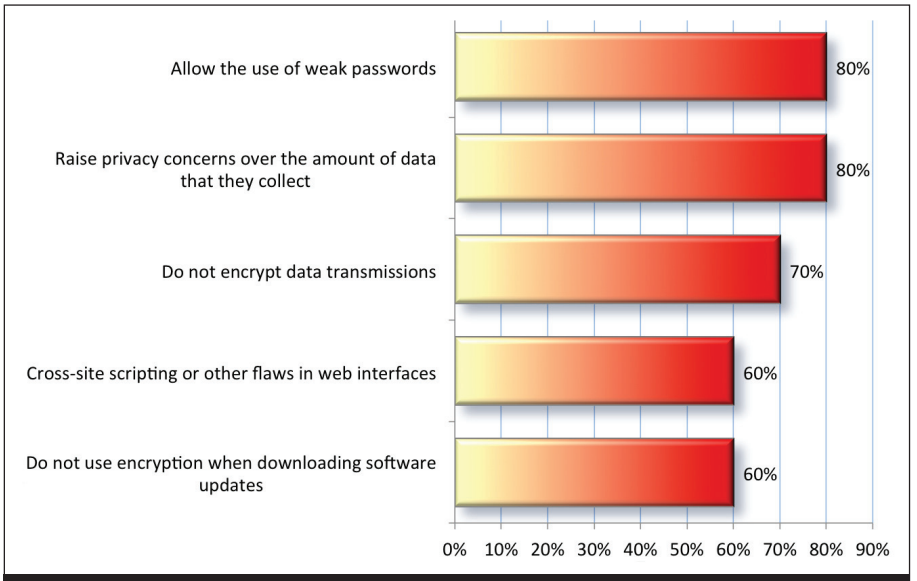


Figure 2: Device-level IoT security vulnerabilities. Source: HP Fortify.

- Insecure web interface.
- Insufficient authentication/authorisation.
- Insecure network services.
- Lack of transport encryption.
- Privacy concerns.
- Insecure cloud interface.
- Insecure mobile interface.
- Insufficient security configurability.
- Insecure software/firmware.
- Poor physical security.

This is echoed by recent research undertaken by HP Fortify, the findings of which are shown in Figure 2. Overall, it found that 70% of the most commonly used IoT devices contain security vulnerabilities and there are an average of 25 security concerns per device.

Among the reasons for this is that many IoT devices are not developed with security in mind. Many contain embedded software, often proprietary firmware, which is problematic to patch and upgrade, leading to vulnerability and configuration management issues. Many devices do not undergo any kind of security review. According to SANS, just 52% of IoT devices undergo security evaluations or testing prior to production.

Solving the security challenges

To solve the security challenges of IoT devices, a different stance needs to be taken. Security needs to be built into products by design. It cannot be bolted on afterwards. There are moves, such as the position being taken by the US Food and Drug Administration regarding medical equipment, to encourage manufacturers and facilities to ensure that appropriate security safeguards are built in from the start of the design process, as well as to remain vigilant regarding new risks and threats as they are uncovered. This is especially important since it has already been demonstrated that implantable medical devices such as pacemakers and defibrillators can be remotely hacked and exploits such as changing dosage levels of insulin pumps have been accomplished from a distance of up to 300 metres. As well as this, the University of Michigan has shown that the majority of hospital devices use Windows XP or Windows 95 operating systems, which are extremely vulnerable to computer malware, and many monitoring systems use open wifi connections that can be hacked.

Building in security by design means that controls need to be introduced at the operating system level, should use the device's hardware security capabilities and should extend right up through the device stack to the applications it deploys.

In order to address security throughout the device lifecycle, from the initial design to the operational environment, software vendor Wind River states that there are five essential requirements:

1. Secure booting – the authenticity and integrity of software on a device should be verified via a digital signature attached to the software image and verified by the device to ensure that it has been authorised to run on that device and that there are no runtime threats or malicious exploits present. Only then will it be allowed to load.
2. Access control – mandatory or role-based access controls should be built into the operating system. If compromise of any component is detected, access to other parts of the system should be minimised as much as possible. This will help to minimise the effectiveness of any breach of security.
3. Device authentication – a device should authenticate itself at the point at which it is plugged into the network, prior to receiving or transmitting data. Machine authentication only allows a device to access a network based on credentials that are stored in a secure storage area.
4. Firewalling and IPS – each device needs to have a firewall or deep packet inspection capability for controlling traffic, but this requires that protocols are needed to identify malicious payloads hiding on non-IT protocols. And these protocols need to be industry-specific since – for example, smart energy grids have their own set of protocols governing how devices talk to each other.
5. Updates and patches – the ability to deliver software updates and patches to thousands of devices in a way that conserves limited bandwidth and intermittent connectivity of embedded devices, while ensuring that there is no possibility of functional safety being compromised, is a necessity.

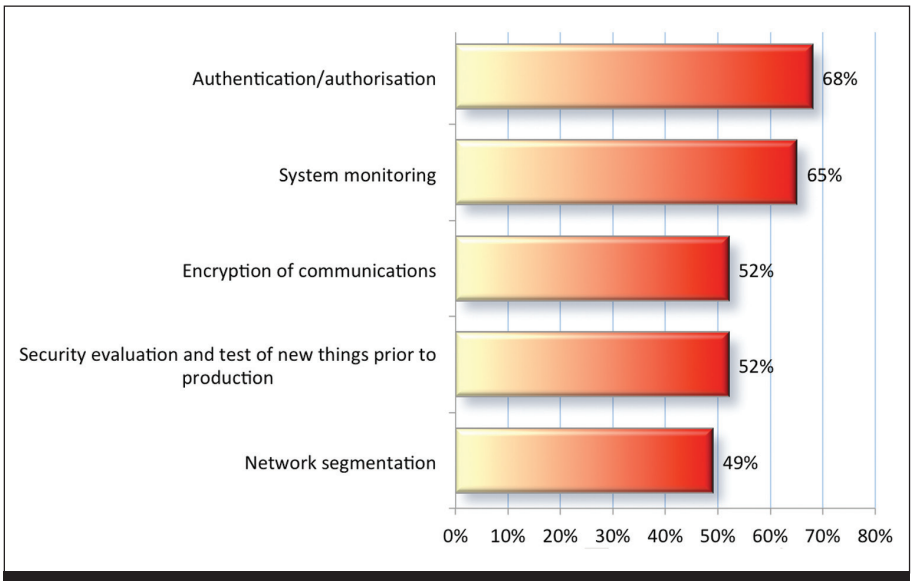


Figure 3: Top controls currently in place for securing the IoT. Source: SANS Institute.

Essential steps

It is unlikely that security will become an over-arching requirement in the design process any time soon. There are also standards that need to be developed before this happens and it is also likely that some form of regulation or specific industry pressure will be required in order to force manufacturers to place the necessary emphasis on security.

Organisations should look to limit what is allowed in the workplace, considering the risks versus the benefits, and look at how systems are interconnected and therefore how risks such as malware infections can be spread.

"Systems will need to be used to link physical and network security together to enable a total view of incidents, enabling management to make decisions regarding the threat posed"

Organisations also need to find a way to enforce data protection policies on all devices in use and to control what data people can access. Identity and access rights should be tightly managed in order that all devices and connections are authenticated and authorised, and controls should be placed on what information can be viewed and how it is communicated and stored. All data held on devices or in transit should be encrypted to safeguard it from unauthorised access or loss. In terms of devices that are lost or stolen, device management tools that extend to remote data wipe should be considered, especially for consumer devices that are personally owned.

For devices used for business operations, systems will need to be used to link physical and network security together to enable a total view of incidents, enabling management to make decisions regarding the threat posed and how it can be controlled. This requires that all IoT devices are managed the same way as other equipment connected to the Internet and the network. All activity should be closely and continuously monitored to look for anomalies from normal baseline behaviour and organisations should ensure that all devices are correctly configured and are operating properly.

Where anomalies are uncovered, organisations need to have workflow and escalation procedures in place so that those in charge of security are alerted promptly to any potentially serious security threat or incident. This will help greatly in the time taken, and therefore cost, for remediating problems. It is

essential that all procedures and processes are documented, completed in a compliant way and an audit trail is generated to provide evidence of the effectiveness of actions taken.

Figure 3 illustrates the controls that organisations currently have in place for controlling IoT devices in the workplace according to the SANS Institute.

Remain vigilant

While it could be said that the IoT is still in its infancy, IoT devices and increased connectivity are being seen across a wide range of sectors. Many will be familiar with consumer-oriented smart, highly connected devices and these are invading the workplace. Organisations are still grappling with the BYOD phenomenon that has an increasing array of personally owned smartphones and tablets being used for work purposes, creating headaches for many in terms of managing them and controlling what sensitive data can be accessed. Now this is being extended to wearables such as smartwatches and health and fitness monitoring devices.

But the industrial IoT holds the greatest promise, offering to improve productivity, ease safety issues and reduce operational costs in a wide range of scenarios and industries.

Organisations would be well advised to thoroughly research the risks involved in each scenario in which IoT devices are deployed and to communicate with employees, partners and customers about security and privacy risks, especially, where sensitive data is at risk. This should include both consumer devices that they wish to purchase and use to interact with corporate information, as well as how devices used, for example, in smart buildings should be closely monitored and maintained. One point of failure in a hyper-interconnected network can initiate a chain of events that could have catastrophic consequences.

The IoT appears to be an unstoppable force and the rising tide of devices cannot be turned back. Until security issues are solved, organisations need to be vigilant, ensuring that they weigh-up the security risks against the benefits to be gained, putting appropriate controls and policies in place, and keeping a constant eye over what is connected to their networks and how devices are performing.

About the author

Colin Tankard is managing director of data security company Digital Pathways which specialises in the design, implementation and management of systems that ensure the security of all data whether at rest within the network, mobile device, in storage or data in transit across public or private networks.

References

1. Manyika, J; Chui, M; Bisson, P; Woetzel, J; Dobbs, R; Bughin, J; Aharon, D. 'Unlocking the potential of the Internet of Things'. McKinsey Global Institute, June 2015 Accessed Aug 2015. www.mckinsey.com/insights/business_technology/the_Internet_of_things_the_value_of_digitizing_the_physical_world.
2. 'OWASP' Internet of Things Top 10 Project'. OWASP. Accessed Aug 2015. www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project.

Big data – the future of cyber-security or its latest threat?


Cath Everett

Cath Everett, freelance journalist

Everyone seems to be talking about big data lately. The much-vaunted ability to analyse large diverse data sets very quickly really does appear to have become the hottest of hot tech topics over the past few years. In fact, big data, despite being such an over-used term, has even managed to worm its way into mainstream public consciousness – mainly because of the insights it has been able to afford by finding patterns in what often appears to be unrelated information.

Killer app

In an industry context, meanwhile, a raft of glowing articles have emerged in the computer press recently extolling the technology's virtues and dubbing it the future of cyber-security – or alternatively claiming that information security is big data's killer app. But is there any truth in such hyperbolic statements? And if so, what is this future likely to look like? As usual, views are mixed.

According to Peter Wood, chief executive of information security consultancy

Peter Wood, First Base Technologies: "It's a nearly impossible task to monitor everything in security terms and it's not always appropriate."

First Base Technologies, big data is definitely the way forward. "For most large organisations, it's a nearly impossible task to monitor everything in security terms and it's not always appropriate," he says. "The issue is that information has now spread everywhere – from the cloud to personal devices – which makes it difficult to decide on what the network perimeter is and how to defend it."

As a result, the challenge these days is less about defending access to the network and the devices on it, and more about preventing access to data. Such a consideration is particularly important in a sophisticated world where any cybercriminals worth their salt are likely to be using legitimate user credentials gained via spear-phishing or other such methods to attack their targets. This situation makes breaches very tricky to identify using traditional means.

"It's very difficult to do any form of meaningful threat detection today, which is why big data offers such big benefits, as it's the next stage in behavioural intrusion detection (IDS) and prevention systems (IPS)," Wood says.

Promise of big data

A key issue with traditional IDS and IPS offerings has always been the requirement for information security specialists to set up, configure and tune them so that they can recognise and alert them to anomalous behaviour, a process that tends to be laborious and time-consuming. Failure to do so, however, tends to result in false positives or problems being missed. Regular system and network logs, on the other hand, tend to be widely ignored unless an incident occurs.

The promise of big data is that it could not only help to detect threats and identify behavioural anomalies in near real-time, but could also, in the future, provide the necessary intelligence to launch an automatic response to an attack.

Such systems work by combining data from multiple sources across the enterprise into one large database and using sophisticated analysis techniques to identify patterns. These data sources comprise not just logs from desktop and perimeter devices but could also include feeds from CCTV, building access systems and even HR applications.

"Looking at many different factors and bringing them all together in one place has been the Holy Grail for information security for a long time," Wood explains. "While some security information and event management (SIEM) providers are already doing this at a humbler level, big data injects it with steroids."

"The more sophisticated the feeds you can give it, the more accurate the output is likely to be"

He gives an example of how such a system could work based on the activity of fictional Fred in accounts. So Fred usually accesses the finance system from his PC in the office between 9am-12pm and 1pm-5pm each day. But one day, he appears to be trying to do so even though he has not been through the office's security gates that morning and has logged on via the corporate VPN from home. As a result, due to what appears to be suspicious activity, an alert is sent to the information security team to check out the situation.

Mike Gillespie, Advent IM: "To provide this level of monitoring in-house would be very resource-intensive."

"Everything becomes more automated with big data and the incident analysis team has a better chance of being alerted sooner and with higher degrees of accuracy," Wood says. "The more sophisticated the feeds you can give it, the more accurate the output is likely to be, especially if you expand it to cover information from buildings or HR databases and the like."

While some offerings exist in this space today in the shape of IBM's Security Intelligence with Big Data suite and BAE Systems' Detica CyberReveal analytics and investigation environment, they are still a long way from becoming off-the-shelf packages or ready-to-deploy cloud services.

New approaches

As a result, uptake has so far lacked momentum. "There are some early adopters and, for major corporations with a sophisticated security posture, I'm sure they're looking at these kind of systems already, but they're not really talking about it," Wood says.

Smaller firms, on the other hand, are unlikely to go for it unless systems are packaged up as commodity products in a similar fashion to anti-virus software, "and they can sign up for £5 per month per employee. But that's a long way away unless someone does something really clever," Wood adds.

Scott Zoldi, FICO: "I believe the industry will move more to streaming analytics."

Nonetheless, it is as a cloud-based service that Mike Gillespie, director of information security consultancy Advent IM, expects big data to really take off in the information security space.

"A medium-sized network with 20,000 devices – so laptops, smartphones and servers – will transmit more than 50TB of data in a 24-hour period," he explains. "That means over 5Gbits must be analysed every second to detect cyber-attacks, potential threats and malware attributed to malicious hackers – and to provide this level of monitoring in-house would be very resource-intensive."

Another key issue is the general lack of big data skills, whether security-related or not, which makes acquiring such expertise expensive unless you are prepared to train personnel yourself. In fact, a survey by Gartner among 284 of its large corporate Research Circle members, which consists of both IT and business leaders, indicated that 57% considered a lack of available big data skills to be the biggest single inhibitor to adoption.

Scott Zoldi, vice president of analytics science at FICO, which has measured consumer credit risk across the globe for at least two decades, believes he has the answer in the form of streaming analytics – not least because the technology operates in real-time.

"Today folks are collecting data, putting it in Hadoop [big data] systems and looking at correlations. It's one approach but it's not real-time and you ideally want to detect a threat as it occurs"

"Today folks are collecting data, putting it in Hadoop [big data] systems and looking at correlations," he says. "It's one approach but it's not real-time and you ideally want to detect a threat as it occurs. So I believe the industry will move more to streaming analytics."

FICO's Cyber Security Analytics system, which was released in February, is based on the firm's payment card fraud detection technology. It uses self-learning analytics and anomaly detection techniques to monitor and look for abnormal activity across both the network and real-time data streams in order to identify and block potential threats.

Self-learning

The fact that the analytics model is self-learning means that it is able to understand what a new attack looks like and how the environment changes in response – and it can refine its activities on that basis.

"It takes streaming analytics models 10 milliseconds to perform a transaction," Zoldi says. "In card fraud, that's what we do to decide whether a transaction is legitimate or not, and the same model is being deployed in cyber-security."

Another advantage of this approach, he claims, is that the system undertakes behavioural analysis of streamed data rather than looking for patterns in persistent data stored in a large database. This makes such data much more tricky to steal as it is not actually stored in a single place.

How the firm's Cyber Security Analytics offering works, meanwhile, is by assigning risk scores to anomalous behaviour based on a set of variables. The technology, which is deployed on an on premise basis, can either be used as standalone system or deployed alongside existing signature-based threat detection systems and SIEM tools.

"In future, security professionals will rely on analytics scores," Zoldi says. "Today they're flooded with alerts. So if they get say 10,000 per day and the team can focus on 1,000 of the highest rank ones, it makes a real difference and means they can concentrate on higher value tasks."

"The opportunity for a security breach with big data is huge, as the data is drawn from lots of sources and stored in one large database"

As he points out, such considerations are particularly important these days in an information security industry suffering from a major skills crisis. "Big data will be a big part of solving the problems we face today, but streaming analytics will potentially be the game-changing technology of the next three years," Zoldi claims. "The issue is that, if companies don't have it, they'll end up being the weakest in the ecosystem and, therefore, potentially vulnerable."

First Base's Wood, however, is unsure whether the technology isn't running before most of the rest of the industry can walk. "The opportunity for a security breach with big data is huge, as the data is drawn from lots of sources and stored in one large database," he acknowledges. "But I don't think that's a block to uptake at the moment because it's so early in the adoption cycle – and most people don't even know enough about it to ask the persistence question as yet."

Rising threat levels

No matter what the most effective response to growing threat levels may prove to be, the need for action is becoming ever more pressing, believes Pete Shoard, chief architect for cyber-security services provider, Secure Data.

A key issue here is that the defence capabilities of government departments and defence suppliers have improved due to "some pretty whizzy analytics". As a result, established state-sponsored actors such as the Comment Crew have started selling on their three-year old but sophisticated malware – which is still undetectable to most commercially available security solutions – to smaller-time criminals, commercial players and hacktivists via the dark net in order to help fund their activities – a useful activity when their government masters are "feeling the pinch".

The Comment Crew, which is also known as the Shanghai Group, has been linked to the Chinese military and is thought to be responsible for many of the country's cyber-attacks since 2006.

"A few years ago, I saw an image placed on a compromised website that contained commands to exercise against the asset in question – it was a very targeted attack," says Shoard. "But a few months ago, I started seeing criminals using the same malware – for example, in insurance companies to traverse inside organisations, this time for commercial gain rather than corporate espionage."

"The danger is that someone with a less ethical mindset combines it with other online data such as the voters' or housing register and is able to form conclusions about individuals"

Organisations that are being particularly hit by this phenomenon include financial and professional services firms as well as telcos, he adds.

Yet another consideration in the big data context is just how to go about securing such systems themselves as well as the data they hold. A key issue here is that big data breaches are likely to be just as big themselves due to the petabytes of data involved – with all of the potential for disaster that implies.

First Base's Wood explains: "The opportunity for a big security breach is huge, but if big data leaks, even if it's anonymised, the danger is that someone with a less ethical mindset combines it with other online data such as the voters' or housing register and is able to form conclusions about individuals. It's when all of this data is combined to make a superset that it gets really scary."

Not well understood

So while all of the usual security rules apply, it becomes more important than ever to ensure that only authorised individuals can access the system, for example. Technologies such as role-based authentication can be useful here, but are not a panacea either.

Wood explains: "At the moment, traditional security controls don't really fit big data sets due to how and where they're stored. So doing authentication can be difficult as it isn't granular enough and tends to offer all-or-nothing access. That makes it difficult if you're sharing with third parties."

As a result of this, over time, he expects technologies such as attribute-based encryption, which is a nascent area of research being actively explored by academics at the moment, to emerge commercially to solve such problems. A form of public key encryption, the technology works by requiring that attributes of a user's key – such as the country in which they live or the kind of subscription they have taken out – matches the attributes of the ciphertext in order for decryption to take place.

The technology is expected to be particularly appropriate to cloud-based systems, something that is relevant in this context given that few organisations are likely to go to the expense of building their own big data infrastructure in-house, but are instead much more likely to deploy it to the cloud.

Multiple sources

A further consideration is that big data systems store and analyse huge amounts of data from multiple sources, including internal databases, web logs and social media content. As a result, ensuring that information is classified correctly and that information owners are identified is very important – even though the process is far from mature in most organisations. While IT would be the most likely function to own the raw data, for instance, business units could well own the final information output, but this situation needs to be clarified.

A final issue to bear in mind is that few people have much knowledge or expertise in this area. Moreover, the small number of early adopters with huge resources that are streets ahead of everyone else do not generally want to talk about their experiences in case it reveals where their vulnerabilities lie.

But as Wood concludes: "The risk with new technology that's not well understood is that it's bound to introduce new vulnerabilities that people haven't even thought of yet, as they simply don't know what questions to ask."

About the author

Cath Everett has been an editor and journalist for more than 20 years, specialising in information security, employment, skills and all things HR. She has worked in the online world since 1996, but also has extensive experience of print, having worked for publications ranging from The Guardian *to* The Manager. *She returned to the UK from South Africa at the end of 2014 where she wrote a lifestyle blog for* International Business Times.

Five seconds to protect your business


Steve Watts

Steve Watts, SecurEnvoy

Data security issues and security breaches within businesses are now a regular occurrence. Everyday it seems that we are hearing about a new cyber-attack or security flaw and just recently it was announced by CEBR and Veracode that cyber-attacks are costing British businesses £34bn a year.[1]

According to the Ponemon '2015 Cost of Data Breach Study', the average total cost of a data breach has increased from $3.52m (£2.25m) to $3.79m (£2.42m) year-on-year.[2] The average cost paid for each lost or stolen record containing sensitive and confidential information has also increased from $145 (£93) in 2014 to $154 (£98) in this year's study.

A recent report from PWC found that nearly nine out of ten large UK organisations have suffered some form of security breach in the past year.[3] This is made worse by the fact that nearly one third of organisations haven't conducted any form of security risk assessment, leaving businesses vulnerable to attack.

The fact that data breaches are costing businesses so much highlights the importance for businesses to act now. In addition to the immediate costs, breaches have further implications such as damage to an organisation's reputation. Once a breach occurs, not only corporate data, but client data is open to attack too. This can lead to costly lawsuits that affect long-term client relationships. After the event, businesses can waste thousands of pounds on reactive and costly audits and hundreds of work hours when cyber-attacks hit.

There is another way

While the knee-jerk reaction is to put in expensive firewalls and tie the hands of eager employees, there is – whisper it – another way. Thanks to the rapid growth of mobile technology, we are all now able to access emails, Internet and apps on the go. Therefore, it actually often makes sense to put employees in control in a world where almost everyone possesses a mobile device. By empowering staff to protect their endpoints, giving them the ability to authenticate their way on their own phone or tablets, budget-conscious and time-sapped IT departments can save valuable time and resources.

"Most people are now used to undertaking their banking, shopping and multiple daily social interactions online, so are well aware of the dangers of bad password management"

Never before have we seen a generation of workers so tech-saturated, yet many organisations are failing to take advantage of this valuable resource, namely by using their employee's own devices as authentication tools to connect, securely, to their business data while on the move.

The belief that employees aren't capable of being trusted to keep their part of the security bargain is outdated. The days of staffers having their password noted down on Post-it notes stuck to their monitors are long gone. Most people are now used to undertaking their banking, shopping and multiple daily social interactions online, so are well aware of the dangers of bad password management and endpoint security even if it is on a subconscious level.

Towards two-factor authentication

The catalyst to this movement towards more trust for your staff is from the emergence of two-factor authentication (2FA), that makes the transition to new devices easier than ever. An extra layer of security, 2FA requires not only a username and password but also something that only the user has on them (ie, a physical token) to generate a one-time passcode (OTP). With digital crime and Internet fraud an increasing concern, such methods of authentication have become increasingly prevalent.

Once only considered for high-end companies (eg, banks), today companies large and small in the government, healthcare, energy, financial services, insurance, manufacturing, marketing, retail, telecommunications, charity, legal and construction sectors are all turning to 2FA for their internal security needs.

The countdown is on

The path to using your staff to secure your systems can take as little as five seconds per user with 2FA:

- Second 1: Unlock your mobile phone.
- Second 2: Open the authentication app.
- Second 3: Select authentication method – pin code or QR code.
- Second 4: Type in code or scan QR code.
- Second 5: You're in.

Using 2FA purposefully is a straightforward and quick process. The simplicity of these steps needs to be recognised by businesses that are looking to address cyber-security. However, a knowledge gap in understanding the benefits is keeping businesses away from utilising this secure process. By correct education and insight, businesses can arm employees and end-users alike with the knowledge and confidence to trust this method and help protect important corporate data from potential breaches.

Emerging threats

It is also important to accept that threats come in many forms and can affect businesses greatly – for example, 15% of large organisations suffered from a security or data breach in the past year involving smartphones or tablets. With increased employee mobility, businesses must equip staff to access corporate data from each of these devices securely.

"Future exciting developments such as near field communication (NFC) will soon empower employees to protect important data and their identity"

In its current state, 2FA is secure and simple to implement; but future exciting developments such as near field communication (NFC) will soon empower employees to protect important data and their identity. This saves even more time because the user doesn't have to open their chosen account or input a username and password. This process will involve a user simply choosing the account they want to activate, entering a four-digit pin and tapping their phone against any Windows 10 PC or tablet device.

Also, in the future, the use of biometric authentication processes will put technology more at our fingertips – literally. RBS Bank recently introduced Touch ID, allowing customers to access their accounts at a swipe of the finger, while Apple Pay has made paying in stores and within apps easier than ever. Google's answer to Apple Pay, Android Pay, provides users with a way to store their payment information locally and make it available securely to third-party apps via API. Gone are the days of searching for cash in your wallet or going into the bank.

"In order for businesses to address the widening threat landscape and protect their changing IT infrastructure, with the increase in uptake of Bring Your Own Device (BYOD), they must assess their security infrastructure"

As you continually read, cyber-attacks are becoming more sophisticated and occurring ever more frequently. In order for businesses to address the widening threat landscape and protect their changing IT infrastructure, with the increase in uptake of Bring Your Own Device (BYOD), they must assess their security infrastructure. And 2FA can provide the peace of mind and protection that businesses require.

With more and more transmission channels becoming available, soon all employees will need to do is select the device that best suits the working environment. Now, and in the future, it is vital that businesses protect important data – this is a key factor in remaining competitive. By implementing a simple five-second security process, a data breach can be avoided, securing important data while protecting assets and avoiding breath-taking costs.

About the author

Steve Watts brings 25 years' of industry experience to his role at SecurEnvoy. He founded the company with Andrew Kemshall in 2003. Before starting SecurEnvoy, Watts was responsible for setting up nonstop IT, the UK's first IT security reseller in 1994. Prior to setting out on his own, he worked as sales director at the networking and IT division of Comtec.

References

1. Tovey, Alan. 'Cyber-attacks cost British industry £34bn a year'. The Telegraph, 10 Jun 2015. Accessed Aug 2015. www.telegraph.co.uk/finance/newsbysector/industry/defence/11663761/Cyber-attacks-cost-British-industry-34bn-a-year.html.
2. Ponemon, Larry. 'Cost of Data Breaches Rising Globally, Says 2015 Cost of a Data Breach Study: Global Analysis'. Security Intelligence, 27 May 2015. Accessed Aug 2015. http://securityintelligence.com/cost-of-a-data-breach-2015/#.VbjYIflVhBc.
3. '2015 Information Security Breaches Survey'. PwC/HM Government. Accessed Aug 2015. www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-02.pdf.

…Continued from page 3
again. However, this is only a temporary solution."

As referenced in the statement, there have been a number of research reports – with the most recent being from MIT – that show how the anonymity offered by Tor can be compromised given the right resources. As Agora's activities are the kind that would naturally attract the attention of law enforcement agencies, such as the FBI, it's likely those resources are being brought to bear on the website.

Conflict among anti-virus firms

A dispute has broken out among anti-virus (AV) software vendors, with allegations of dirty tricks being levelled at Kaspersky.

According to a Reuters story, two unnamed people, claiming to be former employees of Kaspersky, have alleged that the company took harmless Windows systems files, manipulated them to make them look suspicious, classified them as malware and then uploaded them to VirusTotal.

VirusTotal is a service operated by Google that allows AV companies to share information about malicious software. If the allegations are true, other AV vendors may have ended up also classifying the files as harmful. This would have caused their products to produce false positives. At the very least, it would have made the products seem faulty, which could lead to reputational damage and lost sales. And the deletion or quarantining of the files could lead to users' systems becoming unstable or unusable.

The reason given by the two engineers for this alleged gaming of the VirusTotal system is that Kaspersky is annoyed that other AV firms are benefitting from its research. The claim is that some lesser AV firms are doing little more that using the VirusTotal database, and are not engaging in original research of their own.

Also, according to the allegations made by the engineers, Kaspersky reverse-engineered rivals' products in order to see how best to get them to issue false positives. It then shared false information to make their rivals look bad over the course of four years, from 2009 to 2013.

Kaspersky fiercely denies the claims and issued a statement saying: "Kaspersky Lab has never conducted any secret campaign to trick competitors into generating false positives to damage their market standing. Such actions are unethical, dishonest and illegal."

It added: "Although the security market is very competitive, trusted threat data exchange is a critical part of the overall security of the entire IT ecosystem, and we fight hard to help ensure that this exchange is not compromised or corrupted."

Kaspersky has certainly complained about 'copycat' products. In 2010, it carried out a controversial experiment that was not dissimilar to the allegations that have just been made. It took 20 innocuous executable files and classed 10 of them as malware before uploading them to VirusTotal. Just 10 days later, the firm claimed, 14 other vendors had added detection for the 10 files labelled as malware, without making any tests themselves to check that they were, in fact, malicious. This differs from the current allegations, however, in that the uploaded samples were not modified in any way to make them look suspicious. In fact, the whole point was that any real analysis would have revealed them as benign. Kaspersky also announced the details of its experiment shortly after it was carried out.

Kaspersky has also pointed out that it was itself a victim of fraudulent use of VirusTotal back in 2012. The information sharing platform is open to all, and when an anonymous user uploaded bogus files and metadata, Kaspersky ended up misclassifying harmless files from Mail.ru and the Steam gaming platform as malware.

AV firm Dr Web said it has also carried out experiments to test other companies' products. Three years ago it submitted harmless but modified files to a testing laboratory and found that, within days, half of its rivals' products had started to mark the files as malicious. This, according to Dr Web, was because they were failing to apply sufficient quality assurance testing and inadequate whitelisting of benign files.

EVENTS

8–9 October 2015
BruCON
Ghent, Belgium
http://brucon.org

20–21 October 2015
(ISC)² Security Congress EMEA
Munich, Germany
http://emeacongress.isc2.org/

20–21 October 2015
Cyber-security Summit
Minneapolis, US
www.cyber-securitysummit.org

4–5 November 2015
RSA Conference Abu Dhabi
Emirates Palace, Abu Dhabi
www.rsaconference.com/events/ad15

10–13 November 2015
Black Hat Europe
Amsterdam, Netherlands
www.blackhat.com

10–11 November 2015
Information Security Solutions Europe (ISSE)
Berlin, Germany
www.isse.eu.com

16 November–21 December 2015
SANS London 2015
London, UK
www.sans.org/event/london-2015

24–25 November 2015
Info-Crime 2015
London, UK
www.info-crime.com

25 November 2015
Cloud Law European Summit
London, UK
www.cloud-law.eu

29 February–4 March 2016
RSA Conference 2016
San Francisco, US
www.rsaconference.com