ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 April 2018 www.computerfraudandsecurity.com

Featured in this issue:

GDPR puts vendor contracts in the security spotlight

The EU's General Data Protection Regulation (GDPR), which is about to come into force, requires the contracts between an IT department and its suppliers to be reviewed and updated.

However, this needn't be an onerous task. In fact, as David Brook of Turnstone Services points out, successful contract reviews can bring broader benefits. Each contract term relating to data security can be clarified and strengthened as part of a tighter, more comprehensive IT security policy.

Full story on page 5…

Secret digital coin mining and trading is a threat to your business

Coin mining and trading activities by employees – or by hackers – are a huge security problem that every organisation needs to address.

Digital coin software could be infecting your desktops and servers with malware, opening the doors to hackers. They could be after your customer lists, your passwords, your databases. Or they could be looking to turn your computers and devices into bots. Jesse Sampson of Ziften explains the nature of the threat and what to do about it.

Full story on page 8…

Making information security easier

There is a perception that information security is basically some paperwork and a few pieces of hardware, a bit like fitting a burglar alarm to your house.

Alternatively, too many people think that security is too complex and they effectively give up. Luke Briner of PixelPin believes that the current information security environment is too ad hoc, with piecemeal solutions, poorly defined roles and a rat's nest of certification, regulation and law. He makes a plea for greater simplicity and a clearer view of goals and the paths to them.

Full story on page 10…

Multiple breaches leak millions of customer records

Breaches of computer systems belonging to some high-profile brands have resulted in leaks of millions of customer records. In one case the leaks involve payment card details and some of the incidents date back several months.

US sportswear firm Under Armour announced that it had detected a breach of its highly popular MyFitnessPal app in which the personal details of as many as 150 million users had been compromised. Details leaked include usernames, email addresses and hashed passwords, with most of the hashes having been made using bcrypt. This can be effective if it's configured correctly. However, at least a portion of the passwords – probably older records – were hashed with the much less effective SHA-1, which is now considered vulnerable.

Under Armour announced the breach just a few days after discovering it, but it's

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: Bethan Keall

Editor: Steve Mansfield-Devine
E-mail: infosec@webvivant.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. Subscriptions run for 12 months, from the date payment is received.

More information: www.elsevier.com/journals/institutional/computer-fraud-and-security/1361-3723

12986
Digitally Produced by
Mayfield Press (Oxford) Ltd

Editorial

The plot thickens in the spat between Apple and the FBI. It now seems that elements within the FBI withheld information about the agency's ability to crack iPhones because it would have been useful to get a court judgment against Apple and set a legal precedent.

This is what has emerged from an investigation by the US Department of Justice's internal watchdog organisation, the Office of the Inspector General (OIG). The investigation was spurred by concerns raised by people within the agency, not least Executive Assistant Director (EAD) Amy Hess, who was concerned that the testimony she gave to Congress – that the FBI could not crack the iPhone 5C belonging to San Bernardino shooter Syed Farook – was less than entirely truthful.

The FBI demanded that Apple create a special version of the operating system on the phone, iOS 8, so that it could retrieve any data on the device. Apple staunchly refused and the whole matter headed to the courts. But there were always question marks over the FBI's behaviour.

The OIG's report has the eyebrow-raising title of 'A special inquiry regarding the accuracy of FBI statements concerning its capabilities to exploit an iPhone seized during the San Bernardino terror attack investigation'. It reveals tensions between two key elements within the FBI's Operational Technology Division (OTD) – the Cryptographic and Electronic Analysis Unit (CEAU), which is part of the agency's forensics capability and mostly concerns itself with regular law enforcement cases, and the Remote Operations Unit (ROU), which is more normally tasked with national security cases.

Strangely, given how the actions of Farook and his wife were so loudly earmarked as terrorism, it was the CEAU that led the attempt to break into the iPhone. And evidence given by various FBI staff to the effect that it was unable to get through the phone's security defences was accurate, according to the OIG.

It was also strange that the ROU offered no immediate assistance. And while the OIG concludes that it also didn't have the capability to crack the phone, it did have a close relationship with a security company (widely assumed to be Israeli firm Cellebrite, which is not mentioned by name in the report) which it knew was most of the way towards obtaining a crack.

Ultimately, the ROU did approach the security firm and was provided with a means of cracking the phone – just before the case between Apple and the FBI was due to be heard in court. The FBI withdrew the case.

The lack of communication between two key FBI departments is concerning enough. But a murkier picture emerges from the report. It seems the CEAU didn't want a solution to the iPhone problem. In fact, it seems to have gone out of its way to avoid finding one. It seemingly avoided finding out if any branch of the FBI had trusted outside contractors that could help. The ROU acted on its own initiative in sourcing the crack.

"We believe CEAU should have checked with OTD's trusted vendors for possible solutions before advising OTD management, FBI leadership, or the USAO [US Attorney's Office] that there was no other technical alternative and that compelling Apple's assistance was necessary to search the Farook iPhone," says the OIG report.

It seems hard to avoid concluding that the CEAU was more interested in enlarging its legal powers – by obtaining a judgment against Apple – than it was in gathering whatever evidence might have been on the phone. Could this be because the agency already suspected the phone contained no useful information (which turned out to be the case)? Or was it purely engaged in a power play? There are more questions to be answered.

The report is available here: https://oig.justice.gov/reports/2018/o1803.pdf.

– Steve Mansfield-Devine

...Continued from front page

believed the attackers first gained access to the data at least a month earlier. The data affected is fairly limited, although it's possible poorly chosen passwords may be cracked. The company has advised users to change their passwords for MyFitnessPal – and anywhere else where they have used the same password – and to be alert for any emails purporting to come from Under Armour or MyFitnessPal.

A popular bakery and café chain, Panera Bread, which operates 2,100 outlets across the US and Canada, has also potentially exposed millions of customer records. Initially, it was thought that the breach was confined to the firm's customer-facing website, which was taken down temporarily. But it was later claimed that the problem extended to the company's commercial division.

It this case, the breached data was more detailed, including names, email, physical addresses, birth dates, loyalty card number and the last four digits of payment cards. The total number of potentially affected records could be as high as 37 million.

Security researcher Dylan Houlihan alerted Panera that there was a problem with its website leaking data back at the beginning of August 2017. His messages were initially dismissed, but shortly afterwards, the firm said it was working on a fix. However, the website remained online and vulnerable for another eight months. The site was taken down only after Panera was approached by security journalist Brian Krebs. It came online again a little while later with the weakness apparently fixed.

Panera made a statement to Fox News downplaying the breach and claiming that only 10,000 records had been exposed. This was quickly disputed by a number of security firms that pointed out that it was still possible to continue using the flaw simply by registering an account and logging in. At that point, Panera took down its site again.

Luxury department store Saks Fifth Avenue, as well as associated stores Saks Off 5th and Lord & Taylor, have been implicated in the theft of millions of payment card details. Research firm Gemini Advisory discovered a batch of card details being traded by a Russian-speaking hacker group calling itself Fin7 or JokerStash on an underground forum. The 'BigBadBoom-2' file, it was claimed, contained details for 5 million payment cards, of which the group was making 125,000 available for immediate purchase.

The theft was confirmed by Saks, which said the details had been obtained during in-store purchases, which suggests that compromised point-of-sale (POS) terminals were used. It's possible the initial attack vector was via phishing emails sent to Saks employees.

Saks said in a statement that: "We identified the issue, took steps to contain it, and believe it no longer poses a risk to customers shopping at our stores." It also claimed that there is no indication that the issue affected its e-commerce and other digital platforms, or other stores.

"Once we have more clarity around the facts, we will notify our customers quickly and will offer those impacted free identity protection services, including credit and web monitoring," said the company. "We encourage our customers to review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognise."

At the time of writing, it was being reported – although not confirmed by Saks – that a further 1 million card details may have been stolen through Saks stores in Europe and Asia.

Meanwhile, hackers appear to have had access to customer information from Delta Air Lines and department store Sears after a data breach at a third-party service provider.

The firm – [24]7.ai – which provides online chat capabilities for organisations' websites, told its clients that there had been intrusions into its networks in either late September or early October last year. Stolen information included "certain customer payment information", according to Delta. The airline isn't yet sure how many customers may be affected. For its part, Sears believes that the hackers gained access to payment card information for something under 100,000 customers.

On the positive side, the latest 'Threat Intelligence Index' from IBM X-Force says that the number of records leaked as a result of breaches in 2017 was around 4 billion, which is actually a 25% drop compared to the previous year. That said, much of the difference can be attributed to cyber-criminals switching to ransomware attacks, says IBM. The report is here: https://ibm.co/2q6R9ja.

Grindr criticised for sharing data

As Facebook continues to reel from revelations about the way it has allowed third parties to exploit its users' data, gay dating app Grindr, which has 3.6 million daily active users, has joined the ranks of firms accused of over-sharing.

The Norwegian non-profit research organisation Sintef was commissioned to investigate the use of Grindr data by Swedish public broadcaster SVT, which first revealed the issue. Sintef discovered that the service has been sharing users' data with third-party analytics firms Apptimize and Localytics, which help online services optimise their apps.

The shared data includes extremely personal information, including users' HIV status, dates of their last HIV tests, GPS location, email address, phone ID, ethnicity, adherence to certain gay sub-cultures and more.

Grindr stated that it believed it was doing nothing wrong – that these optimisation services are used by many online services and that the data is not used other than to improve Grindr's own services.

"Grindr has never, nor will we ever sell personally identifiable user information – especially information regarding HIV status or last test date – to third parties or advertisers," said Scott Chen, CTO of Grindr in a statement. "As an industry standard practice, Grindr does work with highly regarded vendors to test and optimise how we roll out our platform. These vendors are under strict contractual terms that provide for the highest level of confidentiality, data security and user privacy."

However, it appears that much of the information (except the HIV-related data) has also been shared with third-party advertising firms, often in vulnerable plain-text files. Users have a choice as to whether they provide HIV information, but it may not be clear to many of them that, if they do, this information may be shared beyond Grindr itself.

In brief

Secret Service warns of card scam

The US Secret Service has issued a warning to financial firms about a scam involving chip-enabled debit cards. It seems that criminals are intercepting deliveries of cards and swapping the chips with those taken from old and defunct cards. As soon as the organisations activate the new cards (which won't work) the criminals use the chips – now mounted in the old, donor cards – to withdraw large amounts of money. The crooks are targeting corporate cards because they often have high spending limits. They can't simply use the stolen cards because they have to be activated and that involves knowledge the criminals don't have. It's not clear at what point the deliveries are being intercepted.

BEC the biggest risk…

A report from Proofpoint identifies business email compromise (BEC) as one of the biggest threats facing organisations today. The firm's 'Understanding Email Fraud Survey' found that three-quarters of organisations had experienced at least one targeted email fraud attack in the past two years, and 41% had suffered multiple attempts. More than 77% of firms expect to be targeted by BEC attacks some time in the next 12 months, although only 40% reckoned they have the technology and processes in place to spot them. The Proofpoint report is here: http://bit.ly/2EnhIFL.

…as one football club discovers

Italian football club Lazio has just made the final €2m payment for Dutch player Stefan de Vrij … to the wrong people. The transfer of de Vrij happened a few years ago, but payments were staggered. Just before the final instalment, however, a fraudster pretending to be from the player's former club, Feyenoord, convinced Lazio, via email, that the bank account to which they needed to make the payment had changed. Authorities have managed to trace the funds as far as the Netherlands but, so far, no culprit has been found.

Contactless attack

Contactless fraud – in which criminals use scanners or even smartphone apps to skim the details of contactless payment cards – is one of the most rapidly growing types of fraud. According to UK Finance, it has now overtaken cheque fraud, which totalled £9.8m in 2017. Criminals have made an app available, costing £20, that allows an attacker to read a card's details simply by standing close to the victim. The details are then used to clone the card. However, some banks are downplaying the issue, saying that the cloned cards are worthless without the right chip and the CVV number.

UK police spend little on cybercrime training

Police forces across the UK are spending next to nothing on cybercrime training, according to research by the Conservative-leaning think-tank Parliament Street. In the past three years, North Wales Police spent the most – a total of £375,488, which included a five-day course for 147 people. Cybercrime is also a component of the force's basic training. Gloucestershire Constabulary, on the other hand, spent nothing in that period. The total spend over the three years was £1.3m, in spite of massive increases in online crime. The report, which was based on Freedom of Information requests, is available here: http://bit.ly/2GXGpOF.

Credit freeze firms benefit from Equifax breach

The massive breach at credit-rating firm Equifax last year has generated big business for firms that offer credit freeze services. Many people freeze their credit records as a way of preventing scammers from taking out loans or payment cards using stolen identities. According to research commissioned by loan provider Fundera and carried out by Wakefield Research, since the Equifax breach (although not necessarily as a direct result of it) around a fifth of US residents have frozen their files with one or other of the three major bureaux. The fees for doing so cost the average person around $23, generating around $1.4bn worth of business for the bureaux – which include Equifax. There's more information here: http://bit.ly/2GEIkYU.

Carbanak arrest

The alleged leader of the group behind the Carbanak and Cobalt banking malware attacks has been arrested. A multinational operation, led by Europol and the FBI with the assistance of several national police forces, resulted in the arrest of an unnamed man in Spain. Since 2013, the Carbanak and Cobalt malware has been used to target banks. The Cobalt malware alone led to thefts of up to $10m a time and the total cost of the gang's operations has been put at over €1bn. The malware was often delivered via spear-phishing campaigns that led to the attackers gaining control over a bank's systems. They used this access to remotely infect ATMs from which they would then withdraw cash. The attackers would also make money transfers and modify account details to increase balances on accounts that would then be emptied by money mules. Much of the money was laundered using crypto-currencies. There's more information here: http://bit.ly/2GCkblY.

Swiss banks fear attack

The Swiss Financial Market Supervisory Authority (FINMA) has issued a warning that says cyber-attacks are now the greatest threat facing banks in the country. "The risks connected with these attacks are growing in sync with the pace of global digitalisation. Cyber-attacks are now the most serious operational hazard facing the financial system, and both the private sector and public authorities should take them extremely seriously," the organisation's chief executive, Mark Branson, told Reuters. FINMA has also called for action by the Swiss Government to help bolster the sector's defences.

Mirai-like botnet targets financial firms

A Mirai-botnet exploiting vulnerable Internet of Things (IoT) devices is being used to target financial organisations, according to security company Recorded Future. In a similar manner to the earlier attacks, the new botnet is using the IoTroop/Reaper malware to infect devices that are running with default passwords or no security at all. These include home routers, TVs, DVRs and IP cameras from vendors such as TP-Link, Avtech, MikroTik, Linksys, Synology and GoAhead. The compromised devices are then used to mount distributed denial of service (DDoS) attacks. In January, at least 13,000 devices were employed to attack three financial organisations, with the attack bandwidth reaching 30Gbps at times. There's more information here: http://bit.ly/2GGDpTk.

Vulnerable files

More than 1.5 billion files that should be kept private are accessible over the Internet, according to security firm Digital Shadows. Many of these files contain sensitive information such as payroll data and tax returns. And they are vulnerable because of misconfigured systems. While badly secured Amazon AWS buckets have been hitting the headlines recently, that problem is just the tip of the iceberg, representing a mere 7% of the exposed data found during the research. Poor configuration of networks, especially SMB-based shares, is also a major issue, accounting for a third of the vulnerable files. Other protocols and systems implicated were rsync (28%) and FTP (26%). All told, Digital Shadows found 12 petabytes of data exposed. The report is here: http://bit.ly/2qajMg5.

UK firms vulnerable to IoT attacks

Around 2.7 million businesses in the UK are vulnerable to attacks exploiting Internet of Things devices, according to research by security company ForeScout. This figure is based on a survey of business, which found that 47% admitted to not updating default passwords on all IoT devices when they are added to corporate networks, and 15% admitted to not keeping security patches up to date. To make matters worse, nearly half of the firms were not confident about knowing which devices, and how many, are on their networks.

GDPR puts vendor contracts in the security spotlight

David Brook

David Brook, Turnstone Services

The EU's General Data Protection Regulation (GDPR), which is about to come into force, requires the contracts between an IT department and its suppliers to be reviewed and updated.[1] However, successful contract reviews can bring broader benefits – and to IT security in particular.

In the spotlight

The GDPR programmes that companies currently have in motion are bringing IT vendor contracts into the spotlight. The GDPR changes the regulations surrounding the retention and availability of personal data in IT systems and as the IT ecosystem of a typical business is typically so interlinked with its chosen vendors and service providers, a rethink of the contractual relationships between an IT department and its suppliers is needed. This is to ensure that the processes provided by the third parties are also compliant with the new rulings.

The contract renegotiations associated with the GDPR are closely focused on data security. This article considers a broader review and analysis of vendor contracts and highlights some of the areas where IT vendor contracts tend to be deficient. Eight of the areas we look at impact on IT security. A forensic look at contract terms and a successful review can tighten up these security vulnerabilities and in some cases even make cost savings at the same time. The article concludes by suggesting a strategy for contract review and how companies should focus their attention and renegotiation efforts.

Tighter policy

One of the outcomes of a corporate GDPR programme is that each contract term relating to data security can be clarified and strengthened as part of a tighter, more comprehensive IT security policy.

Reviewing IT vendor contracts is the last step in the process – it logically follows after the earlier stages of a typical corporate GDPR programme:

- Readiness assessment.
- GDPR working group.
- Data inventory.
- Privacy impact assessment.
- Training and awareness.
- Data protection officer appointment.
- Policies and procedures.
- IT vendor contracts renegotiation.

It is at this last stage of the journey, when vendor contracts have been reviewed and updated, that the new GDPR compliant agreements are cemented in place to ensure that the correct services are provided by subcontractors and their contractors.

Red, amber and green

This article examines the findings of a detailed study of 25 real-life vendor contracts that were assessed by CIPS-qualified procurement professionals, rating their completeness and acceptability from the point of view of the customer.

The vendors and suppliers in the review represented various classes of IT vendor: software, datacentre, software support and maintenance, services, telco, hosting, professional services agreements, ICT outsourcing, online cloud services for software as a service (SaaS) and fully managed infrastructure.

In the analysis, the terms of each contract were benchmarked against an established yardstick of what should be present in a fair and equitable contract and were given a simple rating according to how favourable they were to the customer. Where contract terms were acceptable, they were awarded a green light: where they were partly acceptable but deficient in some way they were awarded an amber 'warning' light and where a contract term was seriously deficient or absent – introducing a risk or a business limitation – they were given a red light.

> ***"In the case of 'loss of data', industry best practice requires that the supplier should pay agreed damages for loss or corruption of data. This should be linked to a disaster recovery plan and indemnities"***

The analysts studied the contract terms under 27 key headings governing the cost and service areas of the agreement between the vendor (or service provider) and the customer, and compared them to industry best practice.

For example, in the case of 'loss of data', industry best practice requires that the supplier should pay agreed damages for loss or corruption of data. This

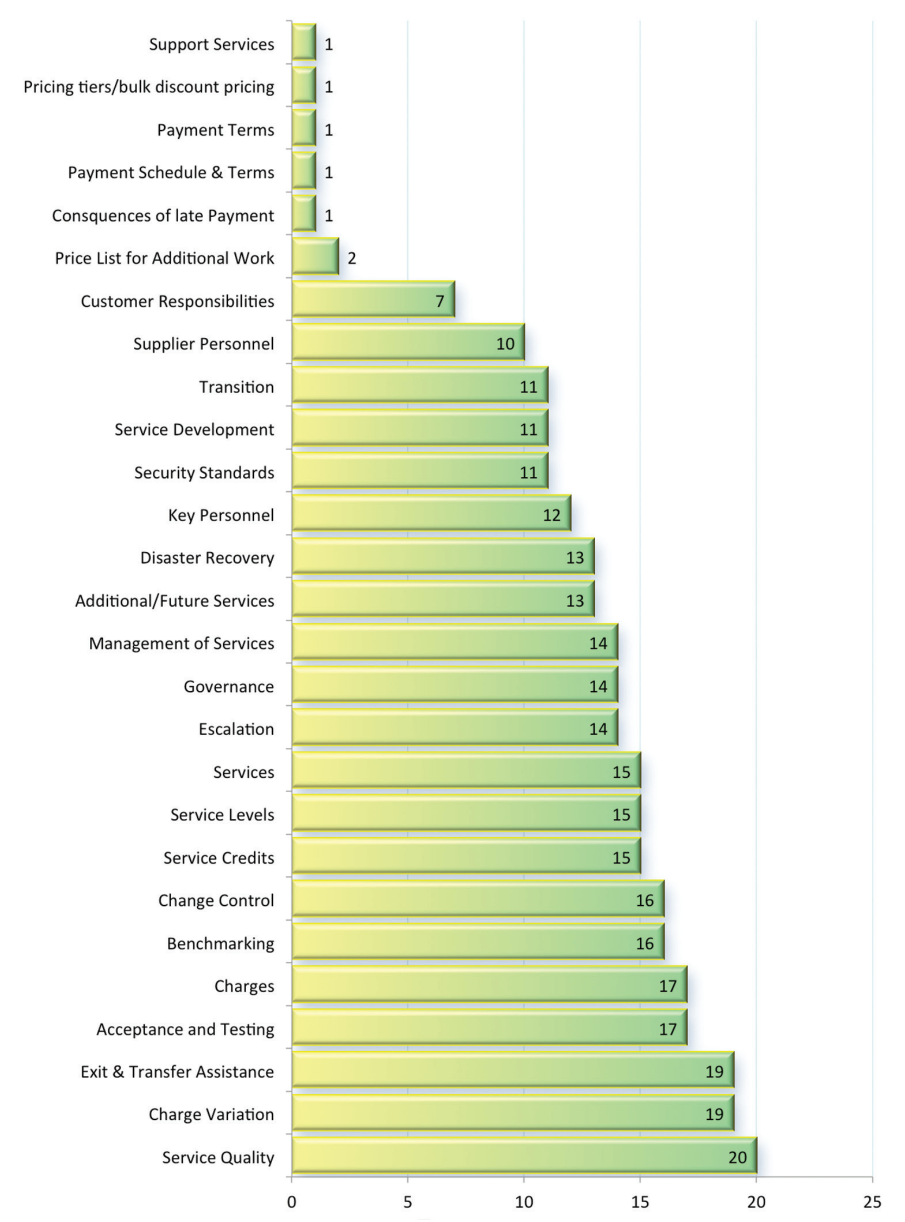


Figure 1: The number of times a contract term was found deficient (awarded a red or amber rating), out of 25 contracts studied.

should be linked to a disaster recovery plan and indemnities. If this point is missing from the contract, the analyst would give the supplier a red light.

Clear picture

The results emerging from the analysis, paint a very clear picture of the contractual areas, including security, that are detrimental to the customer, or unsatisfactory in some way. It's no surprise that suppliers' contracts are worded to suit themselves and it needs more than just a legal resource to identify and then remedy them all.

In the areas that relate most to security – and particularly where contracts relate to subcontractors and their contractors – there were amber warning lights in an alarming number of the contracts studied, particularly in service areas. As can be seen in Figure 1, 50% of the contracts failed to meet best practice for security standards and a worrying 91% lacked detail on service quality. Some of the more general contractual findings were as follows:

Under the heading of 'acceptance and testing', 64% of contracts were deemed to be unacceptable and this heading received the most red lights. Some 77% of the contracts studied were deficient in this area. Services, service quality and service levels also stood out as critical areas where supplier contracts favoured the vendor to an unreasonable degree.

Regarding the important terms surrounding exit and transfer assistance, vendors' standard contracts typically omitted to adequately state their responsibilities and in a surprising number of vendor contracts, this point is missing completely, yet it is particularly important for the customer that the process to exit a contract is clear. It is never too early to define who does what, when and for how much when the exit process is triggered. Both parties need to know what their respective responsibilities are and these responsibilities should be clarified in the clauses relating to customer and supplier responsibilities. However, this is frequently omitted from service provision contracts.

> ***"IT suppliers are often the weakest link in the chain and have been implicated in over half of data breaches, so those aspects of their contracts that represent security weaknesses or liabilities should be assessed with security in mind"***

Clauses on another vital area – benchmarking – are often left out or poorly formed. Depending on the contract type, if benchmarking can be better defined, it may provide cost savings or enhanced confidence in the service being provided.

Software contracts are often lacking clarity for the client in the testing and acceptance terms as well as in the areas of change control and disaster recovery. These are especially important when the software is a mission-critical system.

Contracts relating to fully managed infrastructure services require the services to be performed by the supplier to be listed in detail and without exception.

This is often found not to be the case.

IT suppliers are often the weakest link in the chain and have been implicated in over half of data breaches, so those aspects of their contracts that represent security weaknesses or liabilities should be assessed with security in mind. In particular, this will mean that the clauses that relate to areas such as disaster recovery, security standards, change control, management of services, SLAs and service quality, should be carefully scrutinised to be certain that no responsibilities are overlooked and nothing can slip through the cracks.

Vendor contract review

At the time of writing, the May 25 deadline is fast approaching, so the majority of businesses will be quite far down the GDPR path. The GDPR requires certain points to be covered within the fine print of contracts. While there is a published list of these, they need to be appropriately covered in each in-scope contract.

Many suppliers have template contracts that they use, but often these are not updated. This means that when legislation changes there may be a time lag before the relevant clauses are updated. We have seen this with the Data Protection Act and cloud computing and it is happening again with GDPR – suppliers' standard contracts do not cover it.

External procurement legal experts may open up other points of negotiation, so resource it well. Note that you are also one of many customers in the queue for software suppliers, who are likely to be in negotiations with all their customers on the GDPR.

What is involved in reviewing and re-negotiating contracts? An experienced eye scrutinises the vendor contract terms and makes a cool comparison with best practice, and highlights those that are not acceptable. These will be the target areas for renegotiations. It is a fact that every single supplier contract favours the supplier and not the customer, but it is also true that these terms can be identified, discussed and improved, in terms of security, liabilities and commercial terms.

The huge amount of work that businesses are investing in gaining GDPR compliance may well turn out to be beneficial because it pushes businesses to review their contracts. This is an exercise that they would benefit from doing anyway, first to ensure that contract terms are clear and fair, not weighted in favour of the supplier – it takes a handful of work days, spread over a month or so, to then eliminate any security loopholes.

> ***"It is a fact that every single supplier contract favours the supplier and not the customer, but it is also true that these terms can be identified, discussed and improved, in terms of security, liabilities and commercial terms"***

Although contract reviews may seem onerous, they usually deliver benefits such as better commercial terms and clearer rights and responsibilities, as well as greater protection for the customer. While the GDPR has been a one-off, every company can benefit from re-visiting their supplier contracts, comparing them to industry best practice, clarifying deliverables and tightening up on the security requirements that need to be met.

About the Author

David Brook is co-founder and a director of Turnstone Services (www.turnstone-eservices.com), an IT and procurement consultancy. Since its inception in 2006, the company has addressed over 250 separate vendor contracts, working on behalf of clients within the IT function. The company offers IT vendor contract reviews and renegotiations as a service. Brook's goal is to develop IT procurement as a valued and acknowledged skill in the IT community.

Final analysis

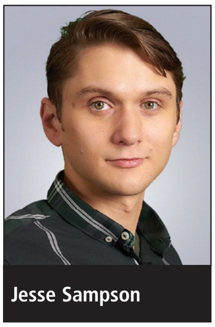
The study of 25 real-life vendor contracts leads to the following conclusions:

- Suppliers have template contracts set up but then never update them.
- Changes in legislation see a lag in suppliers updating the relevant clauses – eg, Data Protection Act, data access (cloud computing), etc.
- Benchmarking is a clause that is often left out or poorly formed. Depending on the contract type, this provides savings or confidence in the service being provided.
- Software contracts are the most poorly formed and lacking in clarity for the client when it comes to testing and acceptance, change control and disaster recovery. This is especially important when the software is bespoke and not out of the box.
- Contracts relating to fully managed infrastructure services require the services to be performed by the supplier in detail and without exception. This is found to be not comprehensive.
- Especially important is how to exit certain types of contract. It's never too early to define who does what and when and for how much.
- Both parties need to know what their respective responsibilities are – who does what and when. Clauses relating to customer and supplier responsibilities will clarify this. These are often left out in service provision contracts.

Reference

1. General Data Protection Regulation (GDPR), home page. Accessed Mar 2018. https://www.eugdpr.org.

Secret digital coin mining and trading is a threat to your business



Jesse Sampson

Jesse Sampson, Ziften

Bitcoin? Monero? Ethereum? It doesn't matter. Coin mining and trading activities by employees – or by hackers – is a huge security problem that every organisation needs to address.

It looks like they just want to make some extra money 'mining' for Ethereum. Harmless, right? Not quite. Digital coin software could be infecting your desktops and servers with malware, opening the doors to hackers who want more than your CPU cycles and your electricity. They could be after your customer lists, your passwords, your databases. They could be looking to turn your computers and devices into bots, ready to spread more malware or launch distributed denial of service (DDoS) attacks. No matter what, it's not good.

The threats might start from your employees, if they choose to try to make a couple of extra dollars, euros, pounds or yen, by mining or trading crypto-currencies. Other dangers could come from hackers, who are hijacking your systems for their own benefit. Let's look at both scenarios.

Unsanctioned coin actions

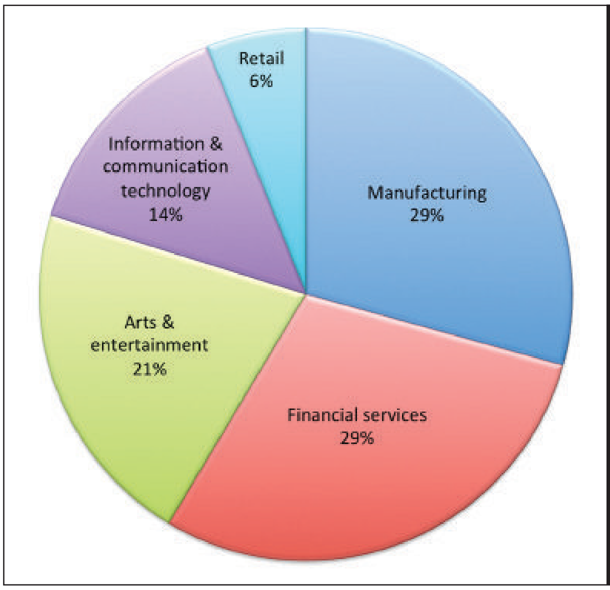
Let's be honest: in most organisations, employees use company-owned computers or company-owned wifi networks to pursue personal interests. Yes, some businesses or government offices are locked down tight. You're not going to see an airline employee checking eBay bids on the PC at the check-in counter. But for many other employees, especially those at desks, a little extra-curricular activity is tolerated, as long as it's not too disruptive or dangerous.

> ***"Working with digital coins is the new day-trading – and should be considered disruptive and dangerous due to the nature of the software that needs to be used for those activities"***

However, working with digital coins is the new day-trading – and should be considered disruptive and dangerous due to the nature of the software that needs to be used for those activities. Every one of our clients has had employees engaged in crypto-currency activities on company computers, like coin mining, coin trading or storing coins on their work machines. It's not good.

There are two types of software that are of interest. One works to mine crypto-coins while the other manages digital wallets. To oversimplify somewhat, coin mining software uses CPU cycles and memory on the end-user's computer to solve very difficult maths problems. The more problems that are solved, the more coins are mined, or created, and added to the end user's account.

Coin mining requires a lot of computing power in order to make a few pennies' worth of crypto-currency. The more powerful the computer, the faster the employee makes money. If the employee can manage to harness multiple desktop or notebook computers – or more powerful computers, such as corporate servers or cloud resources – he or she makes even more money.



The top-five industries targeted by coin-mining attacks. Source: IBM Managed Security Services.

Power costs

There are two dangers here, beyond wasted employee productivity. First, there's the fact that running mining software consumes considerable electricity. It's not trivial. And second, if coin mining software is installed on servers, it's reducing the amount of server processing capability to be used for legitimate work. That means that necessary business applications run slower, or might even be crowded out (and made to fail) by the coin mining software.

Note that these days, it requires too much processing power to meaningfully mine Bitcoin, the best-known crypto-currency. So, employees are mining newer or less-known currencies, such as Monero, Ethereum, or any one of dozens of coins.

Don't underestimate the amount of electricity consumed by coin mining. To get an idea of what's involved, let's compare it to playing computer games. If you use a regular gaming computer and play games for eight hours a day, you'd use 2,000kWh per year of electricity. With mining, it's more like 5,000kWh. That could cost $500 per computer or more annually. A large business might have $10,000 a year in electric bills from illegal coin mining activities.

What can you do?

Here are some ideas for what you can do to counter the coin-mining threat:

- Make sure your anti-virus software is up to date on all corporate assets and that your AV solution blocks coin software: contact your vendor to make sure.
- Don't allow non-corporate devices to access the enterprise network – and that includes personal devices, such as the employee's personal computer brought into the office.
- Set strong policies against the use of mining or coin-management software on enterprise devices or in the workplace – treat it as you would pornography or other disruptive and dangerous software.
- Configure firewall policies to block access to known websites involved in crypto-currencies or which are hubs for the distribution of coin software. This is an ever-changing list, so you must be vigilant.
- Sites to consider blocking include coinbase.com, cex.io, binance.com, kraken.com, etherdelta.com, coindesk.com and blockchain.info.
- Monitor corporate computers to see if they have excessive CPU or memory utilisation, which could be the result of coin-mining software.
- Alert employees that if their computer seems to be running slower than usual, to report this to IT.
- Keep all servers up to date with patches and fixes, to make sure you aren't hosting malware yourself.

And to counter the threat from malicious advertisements:

- Install ad blockers on corporate computers. That's a shame for legitimate advertisers, but your security comes first.
- Double-check anti-virus applications to see if they can detect and block malicious JavaScript or over code running in ads or websites.
- Instruct employees to only use browsers that have been approved by IT as being resistant to ad hijacking.

Digital wallets

You may have read that digital wallets, which are used to manage digital currency accounts, have been targeted by thieves, who break into systems to capture the coins. If those wallets are on your company-owned computers, hackers are breaking into your own resources, including your computers, servers or network.

Those digital wallets (and mining applications) aren't carefully written applications by name-brand vendors. They're not from IBM, Microsoft, Oracle, SAP, Google, Amazon or Apple. Instead, these applications are written by heaven knows who, often an anonymous source and distributed via questionable means – including the dark web. To get the software for crypto-currencies, you have to go into bad neighbourhoods. You have to go to websites targeted by hackers and you're downloading questionable software that might be faked.

For example, take EtherDelta, a coin exchange marketplace that was taken over by hackers in December 2017 by subverting the website's DNS information.[1] This allowed them to steal Ethereum coins and do man-in-the-middle attacks. Hackers got hold of the Github account and used it for malware.

Because crypto-currencies fly under the official radar, many of the applications used to manage digital coins and accounts are easy hackable, or contain built-in back doors. In some cases, the coin software's functionality is a trojan, designed to allow hackers to explore local computers and networks, or take over systems via malware. That malware could be used to steal the contents of an employee's computer, explore the network and possibly spread and infect other systems. It can also be used to turn computers into bots, invisibly controlled by hackers and used to carry out DDoS attacks on external targets.

Outside hacking

As we've seen, hackers can try to subvert your employees' coin-mining and coin-trading activities via malware installed in coin applications. The payoff for them could be the coins themselves, or it could be the ability to penetrate corporate networks.

But there's another danger that's been detected only recently – the use of malicious JavaScript or malicious ads to do some of the calculations needed to mine software, but this time on the hacker's account. Software on web pages use the end-user's computer to perform calculations all the time. Those actions can be delivered via JavaScript, a programming language used to embed client-side applications into the browser, whether it's Firefox, Chrome, Internet Explorer, Safari or Edge. Most JavaScript is fine and makes web pages more interactive and responsive. However, JavaScript can also be malicious.

"Think about every ad that displays an animation designed to get your attention – it's running some code on your computer. Is it 100% safe? There's no way to know"

The same is true of embedded advertisements. An ad, purchased on a media website such as YouTube, is most likely legitimate – or it could be a front for malware that runs on the user's computer, even if the user didn't click on it. Think about every ad that displays an animation designed to get your attention – it's running some code on your computer. Is it 100% safe? There's no way to know.[2] Modern browsers do a pretty good job of keeping ads from gaining access to files on your computer or network, or from installing malware, but those ads can still use up memory and processor time to mine coins. What's more, if the employee clicks on them, the ad might try to install malware.

A challenge here is that your employee might not be doing anything wrong. While malicious ads are common on unsavoury websites (most notoriously on pornography sites), they also appear on what should be trusted, genuine websites. According to one researcher, this so-called crypto-jacking software was found on nearly 2,500 e-commerce websites.[3] And IBM's X-Force security team has documented the use of coin-mining software hidden inside web servers running Joomla or WordPress content engines, which can use the website visitor's website to mine coins.[4]

Never-ending battle

As with all malware and cyber-security, we're playing a game of whack-a-mole. Fix one problem, another pops up. Fix that problem, and oh, look, now there's coin-mining and coin-stealing. Be aware of the coin issue and foster a culture of security. We have beaten other security epidemics and we'll get this one too. And then, of course, we'll need to find the next pop-up mole that needs to be whacked.

About the author

Jesse Sampson, Ziften's director of analytics, brings to bear years of experience applying a variety of analytic methods – from traditional econometric analysis to modern machine learning techniques – across diverse industries. As a data scientist, he has made data do useful things for customers, stakeholders and partners in health care at 21CT, in workforce and education at the Texas Workforce Commission, and public relations at top Austin consultancy Vianovo before finally finding a new passion in cyber-security at Ziften. He has also delivered results as an analytics consultant for major companies in air transportation and logistics. Sampson holds a bachelor's degree in international relations and Chinese from Kalamazoo College and a master's in public policy analysis from the LBJ School at The University of Texas at Austin.

References

1. Schroeder, Stan. 'Crypto-currency exchange EtherDelta got replaced with a fake site that steals your money'. Mashable, 21 Dec 2017. Accessed Mar 2018. https://mashable.com/2017/12/21/etherdelta-hacked/#n30pOLGPbqqM.
2. Goodin, Dan. 'Now even YouTube serves ads with CPU-draining crypto-currency miners'. Ars Technica, 26 Jan 2018. Accessed Mar 2018. https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-crypto-currency-miners/.
3. 'Cryptojacking found on 2496 online stores'. Gwillem's Lab, 7 Nov 2018. Accessed Mar 2018. https://gwillem.gitlab.io/2017/11/07/cryptojacking-found-on-2496-stores/.
4. McMillen, Dave. 'Network attacks containing crypto-currency CPU mining tools grow sixfold'. SecurityIntelligence, IBM, 19 Sep 2017. Accessed Mar 2018. https://securityintelligence.com/network-attacks-containing-crypto-currency-cpu-mining-tools-grow-sixfold/.

Making information security easier

Luke Briner, PixelPin

Luke Briner

For too many people, information security makes their head hurt. At best we can keep a light grip on a small part of the risk base, but at worst it feels like trying to climb a greasy pole. For every strong movement upwards we end up feeling like we know less than we did before. How is that possible? Just like being a doctor, lawyer or tightrope walker, working in information security is hard. Very hard.

There is a perception in the general workforce and public that information security is basically some paperwork and a few pieces of hardware, a bit like fitting a burglar alarm to your house. How hard can it be? How on earth could TalkTalk, Equifax, Sony and all those other breached companies fail their customers so badly?

"A designer might be able to produce good designs without formal education but can we really carry on allowing just anyone to set up a 'web design company' writing production systems that are storing user data, processing card transactions and so on?"

Hopefully, all of us know that despite some mistakes made by these companies, most of us could have been in the same position – perhaps some of us already are. So let's discuss some of the reasons why information security is difficult and, by taking a step backwards, give some suggestions about ways in which things must change if we are ever to move away from a reactionary industry to an effective and proactive one.

Large arena

Information security (IS) is a very large arena. Currently, most IS professionals are expected to be experts in everything; but that's like thinking that all engineers are experts in electrical, mechanical, chemical and civil engineering. I am an electrical engineer and know precisely nothing about civil and chemical engineering. Why would I?

In the IS world, however, what we have not done effectively as a profession is to clearly segment areas of expertise so that you can be, for example, a 'network security manager', where that means something specific like 'electrical engineer'. There are some elements of this within certain organisations but these are not defined roles and can end up crossing over. Is the network manager in charge of security on our web applications? Just the network bits? Is that the role instead of the application security engineer? Like most things, having something to begin with, even if not perfect, is better than being entirely ad hoc.

One problem you see frequently is the lack of formal education or qualifications required to enter the world of digital. Sure, a designer might be able to produce good designs without formal education (even if it would still help) but can we really carry on allowing just anyone to set up a 'web design company' writing production systems that are storing user data, processing card transactions and so on?

An example encountered recently is that of a system a colleague saw that is still in use at airports and which could be used trivially to dump information onto TV screens such as bomb hoaxes or other inappropriate content. Why is it easy to hack? Because it was written by people who didn't really know what they were doing. It's not uncommon for developers to know virtually nothing about web application security. Does training guarantee they would know more? No, but it would certainly put things on the radar for most organisations, since a single person is all it takes to bring something good to the wider team.

"Should we insist that a company is not allowed to write applications that store personal data, operate on safety-critical systems or sit alongside those that do unless they have an appropriate certification?"

At least at management level, most people will have an accreditation, but should this be a legal requirement if we are to take the trade seriously? We would be mortified to hear that a doctor operating on us was not qualified because, 'they taught themselves and know roughly what they are doing'. For some reason, this has happened to our industry and we need to improve things: even if we can only directly affect our own company initially, we probably need to lobby governments to regulate the industry more, at least within certain parameters.

Training and education

The world of training and education also needs to get involved. We already have accredited courses. If you want to be a chartered engineer, a doctor, a lawyer or accountant, you have to pass certain exams after doing specific training. These are maintained by the industry and government departments to ensure standards are upheld – but in our industry, not so much.

Should we have accredited diplomas, degrees etc? Should we insist that a company is not allowed to write applications that store personal data, operate on safety-critical systems or sit alongside those that do unless they have an appropriate certification or the project is signed off by someone with one? Could we not require that the head of IS in an organisation must have an accredited qualification but also team leaders, design authorities, even the 'chief application security officer' who could be the one who is in charge of application security legally and must have an accredited qualification?

Of course, some in the industry would complain that it is hard enough to recruit as it is, let alone with this requirement. That cannot be an excuse, however, for not fixing something that is broken. Again, the trick would be to do something now that at least fixes part of the system and improves it as the industry has time to adjust.

Ad hoc environment

Managing information, sorting the old from the new, the good from the bad, the relevant from the irrelevant is basically impossible in the current ad hoc environment we work in. Take an example: if you want to understand GDPR2 regulations and do a Google search, you will get 5.7 million results. In this case, the top results look promising – the EU site and the UK site, followed by Wikipedia and a lot of other people trying to be helpful. Why so much information? Because if you write a helpful article on GDPR, people might come to your site and buy your legal services or invite you to a conference or maybe you will get ad revenue. Alternatively, perhaps the official sources are far too terse and impenetrable for us mortals to understand.

This problem exists in some domains much more than others. Search for a programming problem and you will get thousands of hits, some of which you do not know are relevant, some might be good or even good *if* you are doing it in a certain way. Maybe it used to be a good way but not any more. It seems there is no general movement to sanitise and score the information that we are trying to use to do things properly – everyday questions, especially for newbies, such as regulation, industry best-practice, new technologies, software vulnerabilities and so on. How many of you know whether you are running vulnerable software like Equifax was?

> ***"It seems there is no general movement to sanitise and score the information that we are trying to use to do things properly – everyday questions, especially for newbies, such as regulation, industry best-practice, new technologies, software vulnerabilities and so on"***

The current 'best' solution is that someone comes along and thinks they could aggregate the data for us to use. Which is great, unless they are also pulling in bad data and not following updating advice, as well as the fact that multiple people always attempt to fix the same thing. Want advice on ISO27001? Good luck. This is a much harder problem to solve, of course. The information does not belong to any one person, although the search engines could potentially do something with listings to help us find what we need.

What we really need is a creative solution – something different. Rather than trying to reorganise the mess, how do we rethink it? How do we get governments, industry bodies and so on to recognise that people need several different formats of the same information – the newbies' guide, the outline, the cheat-sheet and the full-blooded lawyer-pleasing regulation? Perhaps if these were produced well, the demand for these other unsolicited 'help guides' would diminish. We need to get the authors of these help guides to provide metadata that helps the search results to expire or to correctly categorise information rather than the web 1.0 'trick' of trying to put it into as many categories as possible.

Legal regulations

One of the areas that is discussed frequently, especially after a major breach, is the role of legal regulations. How can countries legislate to protect people from poor security? Unfortunately, with the current state of information security as discussed above, the answer is, 'not very easily'. Could Equifax *theoretically* have dealt with the known vulnerability in its web application and prevented the breach? Yes. Was it criminally negligent in not doing so? Probably not – in the same way that most of us would not be happy about ending up in court because our Windows 10 machines were not up to date and some CPU bug was leveraged for an attack and we 'knew about it'.

There is also a problem about borders, which are more easily respected in legislation than they are in the digital world. The Pirate Bay used the lack of copyright laws in Sweden to avoid the US authorities. And even if it was breaking laws, all it would need to do is to locate somewhere where enforcement is hard or expensive and it could continue to do things on the cheap and without the protection that could be offered by a law.

That isn't to say that a government couldn't introduce some kind of accreditation like we have for window installers or gas fitters. This would be a badge that effectively says, 'you could theoretically go to someone else but if you did you would not be insured and would potentially be committing a crime'. Perhaps that would be a way to push suppliers into taking their craft more seriously. Potentially, this badge could be acquired by a web application framework or piece of vendor hardware so that if used in accordance with instructions, you are automatically covered. Only if you start customising it or modifying it outside of known parameters would you be liable for ensuring that your own staff had the relevant qualifications.

What can the industry do? What can our companies do? What can the industry organisations do? To start with, we need to be cautious about reinventing the wheel and creating something else to throw into the large pot of information we already cannot handle. In a famous cartoon there are 14 competing standards and someone says, "It is ridiculous that we have so many – we could create a single universal standard to replace them". What happens? You end up with 15 competing standards.

Any new work should be co-ordinated at as high a level as possible. Contact one of the industry bodies or your local government representative. Talk about the problem. Is your solution a good idea? If so, can it be done in a publicly visible way so others know that you are already solving the problem? You might be surprised at what is already happening but which you simply can't see.

At the coal face

What can you do? You and your team might be the lowest level operatives. You are going to see the coal face with all its challenges and horrors but you are not usually placed in a position of enough authority to directly improve things. The best advice is to learn to step back, something that not all engineers and managers are good at. Is the problem that there is competing advice for GDPR or is the bigger problem that knowing generally what is and isn't true is difficult? Solve the second and you might solve the first. Learn what is foundational and what is noise.

If you find it hard to configure a piece of XYZ equipment, that is not a high-level information security problem that needs solving. If the problem, instead, is that configuring *all* types of network equipment is hard, expensive or error-prone then maybe there is a general problem that needs solving by the manufacturers.

> ***"Software as a service is great for many reasons – it can be maintained and updated in a single place and it can be scaled for higher numbers of users more easily than a hosted system"***

Make sure you play nice with one another. A manager's problems are not a worker's problems but that doesn't mean you have to argue about it. Communicate so that the worker knows that, for example, you are under pressure to deliver because a customer is threatening to go somewhere else, rather than saying 'just get it done'. You might be surprised that some of your workers come up with creative solutions if they know what they are trying to achieve. Likewise, if you are a worker and your manager is telling you to do something, by all means politely question whether X is better than Y; but if you tell them the risks and they still do what they want to do, that is on them – don't make it a problem, you need a good team in the proactive and reactive phases of IS and the last thing you need is bad feeling among the team.

What many newer industries lack are creative solutions. There are some areas where things have been generally modernised. For example, software as a service has delivered robust solutions to many companies in areas of customer relationship management, accounting, HR and others. Software as a service is great for many reasons – it can be maintained and updated in a single place and it can be scaled for higher numbers of users more easily than a hosted system. Now that most parts of at least the developed world have 24-hour Internet access, it is no longer unacceptable to have a system that requires a working Internet connection in order to be used. But as good as those improvements are, they are really an evolution of what already existed and since the light bulb was not invented by continuous improvements of the candle we need to encourage more lateral solutions to the things we struggle with. So let's look briefly at two such ideas and the problems they solve.

Hiding email

The first idea is that we can easily hide email addresses from companies who abuse the information by being overly presumptuous about how many emails they can send you (and sometimes the unsubscribe links mysteriously don't work) or where their business model is to sell the information to others who will send you a ton of marketing information. Conferences can be great, but these are another route for your email address to get to more people than you can control.

There are authentication as a service offerings that use pictures instead of passwords and these can provide a mechanism that does not provide an email address to the organisation when a user logs in but instead provides an opaque key – basically a randomly generated number.

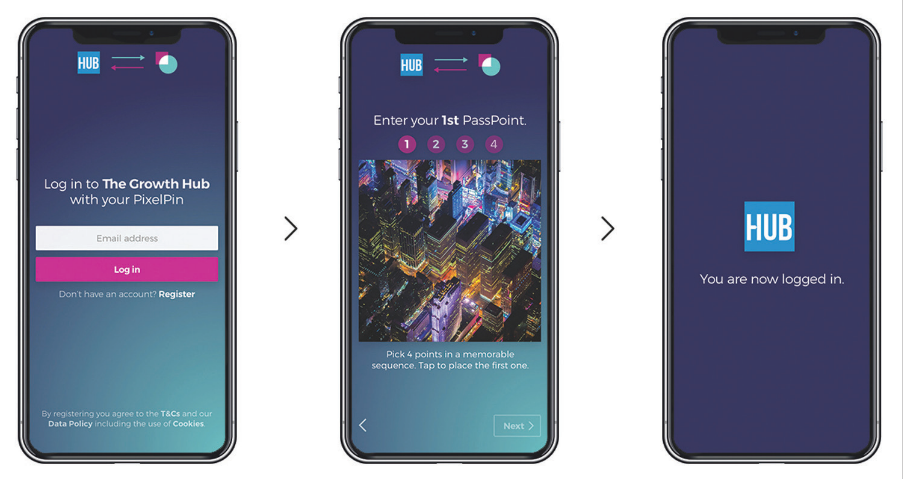
The only way for the company to contact the user is to use the service supplier's API endpoint, authenticate as themselves and send the message with the opaque key. This way, not only can the system hide the email address of the end user from the company, it can also track who is really sending emails (if the sender is not obvious from the content).

> ***"One of the things that shocked most people about Equifax was not that it was breached but that this company, that most people had never heard of, had their private information – lots of it"***

The user can report anyone abusing the sending of emails and the service can easily revoke access either for the company or for a specific user to prevent abuses. Passing this token onto another company will not work unless you also pass your authentication credentials, which could work, except the first company would still be seen as the source of the unsolicited emails and could be sanctioned.

The over-sharing problem

The second idea is to solve the problem of over-sharing private data and thereby increasing the risk of data theft. One



Log in to The Growth Hub with your PixelPin

By registering you agree to the T&Cs and our Data Policy including the use of Cookies.

Enter your 1st PassPoint.

Pick 4 points in a memorable sequence. Tap to place the first one.

You are now logged in.

Some authentication as a service offerings use pictures instead of passwords.

of the things that shocked most people about Equifax was not that it was breached but that this company, that most people had never heard of, had their private information – lots of it. How does it happen?

Institutions that lend you money or provide credit want to know whether you are a reliable customer. They do this by passing the details they collect from you to a credit agency that does this on behalf of so many other institutions that between them they can provide some assurance as to whether you should or should not be lent money. What actually happens is that a company can pay these credit agencies to send them your data – about other borrowing, about address history; it's a large dataset. Even if you don't have a relationship with the end user, you can still buy this data.

The reasoning is sound enough, it is just the implementation that is very risky. We trust institutions like banks not to lose data but it is certainly not guaranteed that it is safe. And if it was stolen, would you know? If you don't like this arrangement then don't borrow anything – no credit cards, no mortgages, no loans and no mobile phones. This is basically not an option for most of us.

So how do we provide the needed outcome without the risk of data sharing? The solution is something we call 'inversion of responsibility' or 'inversion of control'. Rather than an organisation asking the credit agency to send it all of your information, it instead sends the credit agency the lending 'rule' that it will run on the data. The credit agency runs the rule itself and returns the result to the organisation without the latter ever having to see any private data.

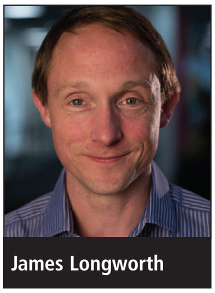
This solution wouldn't have helped with the Equifax breach but if far fewer organisations need to see the private data, the risk of it being stolen is massively reduced. The same basic principle could and should be used with authentication as a service where, instead of collecting customer data yourself, you trust a specialist company to do it for you. It provides the information during a session, so you can get delivery addresses and so on. But as soon as the customer logs out, the information is deleted or anonymised and your risk is removed.

Perhaps you have other ideas? Make them happen, make sure they live in the correct domain – industry, legal, corporate – and let's try and make our industry slightly less hard.

About the author

Cyber-security expert Luke Briner has a strong white-hat hacker pedigree and a passion for electronics. CISSP certified with special expertise in software security, he is the CTO at PixelPin, a company that offers a personalised two-factor visual authentication solution.

VPN: from an obscure network to a widespread solution



James Longworth

James Longworth, Insight UK

Looking at the evolution of virtual private networks (VPNs), one can see a clear shift in their usage in the past decade or so. While VPNs used to be reserved for big companies and government authorities – proving a mystery or unjustifiable expense to most – today we see VPNs being implemented and talked about on a much wider scale. From organisations of all sizes to individuals, more and more people are turning to VPNs to safeguard their data and ensure privacy.

However, to understand what key benefits this technology provides its users, we must first look at how it works. In short, VPNs are used to protect data from being accessed or altered as it travels over another network (eg, the Internet). This is possible through the use of a wide variety of computer protocols that securely 'wrap' your data in a layer of encryption and ensure that the destination for that encrypted data is authenticated (ie: the person or system is who it says it is) and authorised (allowed) to 'unwrap' it. In other words, VPNs allow users to securely access a private network and also share data remotely.

The rise of VPNs

The rise of VPNs goes hand in hand with the rise of other technologies that require a higher level of cyber-security protection. For instance, the sudden rise in popularity of virtual private networks and their current ubiquity is down, in part, to the rise of technology trends such as the Internet of Things (IoT) and bring your own device (BYOD), as well as legislative changes that allow state bodies to require ISPs to monitor and log individuals' online activity.

With more and more entities using these technologies on a daily basis, an increasingly larger number of individuals and organisations have begun to turn their thoughts towards the benefits of VPNs.

Initially, virtual private networks were created to provide secure remote access to network resources. With time, however, the VPN industry has undergone a shift in its focus to allow the technology to accommodate modern necessities. One way of doing this was by making privacy its primary role and unique selling point.

"The VPN industry has undergone a shift in its focus to allow the technology to accommodate modern necessities. One way of doing this was by making privacy its primary role"

As a result, when it comes to new VPN technologies entering the market in the next few years or so, we are looking to see new encryption methods being incorporated so that the technology becomes increasingly robust. In line with this, there are a number of improvements that can be incorporated to facilitate this shift towards a more privacy-focused solution. For instance, the next generation of virtual private networks might see improvements in areas such as anonymous tokenised authentication or protocol obfuscation. As a result, we might soon discover a significant change in how online privacy and data privacy on the Internet is enforced.

Because of these potential changes and the technology's prospects on the market, it is easy to imagine a prosperous future for the industry as a whole. Looking at the past few years, the use of this technology has rapidly shifted from targeting specific organisations to becoming widespread. After all, the VPN industry has the potential to bolster Internet security against a number of cyberthreats.

Holding back

Of course, this sudden rise in the popularity of VPNs among Internet users is not inexplicable - we need merely to look back at the significant amount of cyber-security threats discovered last year and breaches that have made the headlines in recent months. The past few years have been marked by cyberthreats and questions around data security, with hundreds of companies of all sizes rushing to develop new solutions to combat online threats.

Similarly to how firewalls quickly rose in popularity, many industry experts predict that VPNs could become the newest trend in just a few years. Users and providers alike must understand and keep note of the fact that even VPNs cannot completely eradicate cyberthreats or ensure absolute privacy for online users but in spite of this, it is likely that VPNs are on the path to becoming omnipresent in the context of business and professional environments, where the need for increased privacy will only grow in the coming years.

In the past few years, we've seen a significant increase in the need for a secure connection, mainly fuelled by the rise of mobile and the increase in policies like BYOD. With BYOD policies in particular pushing for a more flexible approach to home and mobile working, it comes as no surprise that in many cases users may not even know they are using VPN technologies.

That means that while VPN technology itself hasn't changed much since its inception, the way it is managed has changed significantly. VPNs are now quickly entering the realm of mobile device management, providing secure access to corporate resources. Another benefit is the cut in the number of steps users have to follow to gain access to resources, as everything now happens in the background, making the technology much more accessible and easy to use for the wider public. Inevitably, this leads to a more efficient set-up, speedier on-boarding processes and less lost information.

In turn, this change has led to greater flexibility, particularly for those who frequently work remotely and it has the potential to improve productivity, particularly with the expansion of the gig economy and the increased workplace mobility it offers.

Traditionally, a VPN's main benefit is enhanced security. While some users choose from the multitude of email encryption services and software available on the market, increasingly more prefer to trust VPNs to guarantee their privacy.

More in the future

The VPN industry is now undergoing a shift in its focus to accommodate new user expectations, switching its primary role from providing remote access to network resources to guaranteed privacy. Further to this, many industry experts are expecting new encryptions to be incorporated into the new VPN technologies that will significantly change how online privacy is reinforced.

"VPNs are far from a magic pill against all cyberthreats, but they've certainly secured a firm place in the future of most security-conscious organisations"

As such, it is good to see that both organisations and individuals have increasingly better access to such software, but responsible Internet browsing and common sense must stay at the core of online activity. One aspect must be kept in mind: VPNs are far from a magic pill against all cyberthreats, but they've certainly secured a firm place in the future of most security-conscious organisations and privacy-focused individuals.

About the author

James Longworth is the head of solution architecture (modern workplace) at Insight, where he works on solutions that enable increased productivity for professionals in any business or role. In his previous roles at Insight, he helped clients define their strategy and create cross-architecture roadmaps for their IT environments based on business strategies and priorities.

Identity crisis: the disconnect between business and IT executives

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Computer Fraud & Security*

Perceptions about information security threats vary: what one person sees as a major menace another may view as little more than a nuisance. But while it might be normal for one company to regard the threat landscape differently from another, there can be problems when these mismatched perspectives exist within the same organisation. And as Barry Scott, CTO at Centrify EMEA, explains in this interview, if the C-suite is not getting the right picture, that can lead to dangerously skewed priorities and security strategies.

However, it's not all doom and gloom, and C-level executives are starting to understand security issues, Scott believes.

"Over time, there has been a change in attitude and for the better," he says. "It's considered now to be more a business issue than just an IT issue, so things have certainly gone in the right direction. There's obviously still some work to be done, but there's definitely been a positive move and unfortunately it's probably been as a result of some of the higher-profile things that have gone on."

Barry Scott is CTO for Centrify EMEA. He has over 25 years of Unix, Windows and Linux experience working for many major organisations across industry verticals in various infrastructure operations and architecture roles. For the past 11 years, he has been helping organisations manage their identity management and auditing challenges, focusing on security, regulatory compliance and operational efficiency. Scott's current role is focused around enabling organisations to use infrastructure they already own – Microsoft's Active Directory – to control, secure and audit heterogeneous systems, mobile devices and applications, and also providing them with a unified identity service across datacentre, cloud and mobile.

High-profile organisations suffering widely publicised breaches has definitely raised the awareness of risks, says Scott. And one of the consequences of security failures that has increasingly grabbed the attention of senior executives is the damage to a breached organisation's reputation and consequent loss of customers – aspects many of them hadn't given much thought to in the past.

That said, "There's still a big disconnect between what people actually think are the most important consequences of the breach, compared to how they ought to be looking at things in terms of their reputation and so on," he adds.

This disconnect was highlighted in a recent survey by Dow Jones Customer Intelligence and Centrify that found, for example, that 62% of CEOs considered malware as the greatest threat to the organisation's information security while only 35% of senior technical officers (CIOs, CTOs and CISOs) thought the same.[1] There's even disagreement between the business and technical sides over who is responsible for security strategy, with 81% of CEOs saying they are in control while 78% of technical officers think they drive it. They can't both be right.

Follow the money

It's perhaps understandable if senior executives have taken a while to understand the full ramifications of a cyber-attack. Business people tend to focus on the immediate and tangible cost ramifications of any issue and this is often viewed in terms of disruption to the business. Over time, says Scott, the C-suite has been made only too aware of the other costs involved – not least investigation, remediation and legal expenses.

"There's quite a bit of fear, uncertainty and doubt around GDPR at the moment. The breach notification rules and suchlike are going to improve things longer term and I don't think initially GDPR's going to be as bad as people are saying"

To this list we can add another looming peril – the EU's General Data Protection Regulation (GDPR), although this may have a silver lining, in part because it is opening executives' eyes to the reality that security is a business issue. Many people obsess about the swingeing fines made possible by the regulation, and, says Scott, "there's quite a bit of fear, uncertainty and doubt around GDPR at the moment." But he points out that, "the breach notification rules and suchlike are going to improve things longer term and I don't think initially GDPR's going to be as bad as people are saying."

"A lot of companies are becoming very keen to follow best practice. We've seen a lot more customers wanted to get ISO-certified or, in the UK, Cyber Essentials-certified, because they want to be seen to be doing the right thing"

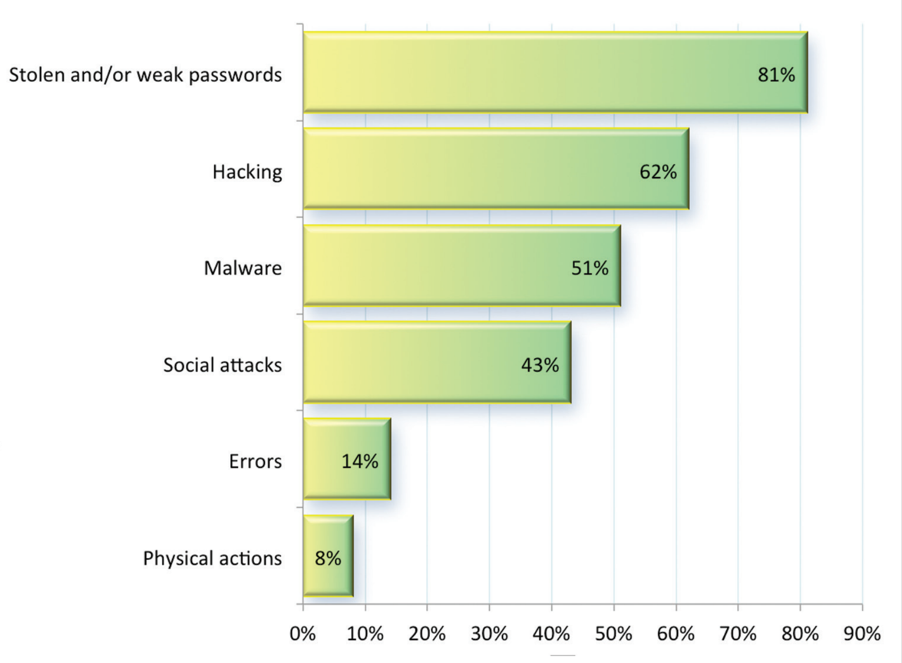
The GDPR doesn't have much to say about specific technical solutions to data protection issues and this is leading organisations to think deeper about how they handle security.

"What has happened is that a lot of companies are becoming very keen to follow best practice," Scott explains. "We've seen a lot more customers wanted to get ISO-certified or, in the UK, Cyber Essentials-certified, because they want to be seen to be doing the right thing. GDPR is seen as a business-level issue."[2]

Chasing the headlines

The fact that cyber-breaches now make the headlines in the mainstream press may be helping C-level executives grasp the importance of the issue, but is it also focusing too much attention on advanced or sophisticated threats and not enough on fundamental security hygiene?

"There's certainly still a situation where, if you get the basics sorted, it will help you out an awful lot," says Scott. "If you don't lock your front door, then it's a bit pointless putting very clever security systems around your house."



Tactics or methods used in data breaches. Source: Verizon DBIR 2017.

Identity problem

Ensuring that your basic security has reached the right level of maturity is important partly because the place where you would once have positioned your defences – the perimeter – has disappeared. And, as Scott points out: "The vast majority of breaches are down to some form of identity problem, and I think that's where the disconnect is actually occurring. As the Verizon data breach report said last year, 81% of breaches were down to weak, default or stolen passwords.[3] So it's really all about identity and access management."

Workers might be accessing your enterprise systems from multiple locations on a variety of devices. You can no longer trust a user based on where they are – a fact that has led to the concept of zero-trust security.

"There's a perception that security gets in the way of people doing stuff. So we're also seeing a requirement that security has got to make your life easier"

"We shouldn't necessarily trust you, just because you're inside the building," says Scott. "You have to do more to identify the actual user, to make sure you know who is making an access request, or that a device is trustworthy – whatever that means in your specific context.

"Then we've also got to ensure that, once we give you access, you can do only what you should be able to do, because we've still got a situation in which far too many people have too much access to too many things from too many places," says Scott. "If you look at a lot of the malware that gets through, ultimately it goes from being inconvenient to really bad news as a result of there being too much privilege involved."

Too complex

In a world of cloud services, mobile devices, remote connections and application APIs, is there a sense that technology has outpaced conventional approaches to security?

"Exactly," says Scott. "There's a very good chance that most of us aren't going through that firewall, that blinky box that we've spent a lot of money on. I don't go through a Centrify firewall from one month to the next because I'm accessing SaaS services from outside the network. So again it comes back to the fact that outside and inside are meaningless concepts today.”

As well as validating users and devices, Scott believes that multi-factor authentication has a big part to play, although there can be push-back from users.

“There’s a perception that security gets in the way of people doing stuff,” he says. “So we’re also seeing a requirement that security has got to make your life easier.”

Traditionally, security has always been perceived as a barrier or a chore – something that slows you down. But here’s where new technologies can provide the solution.

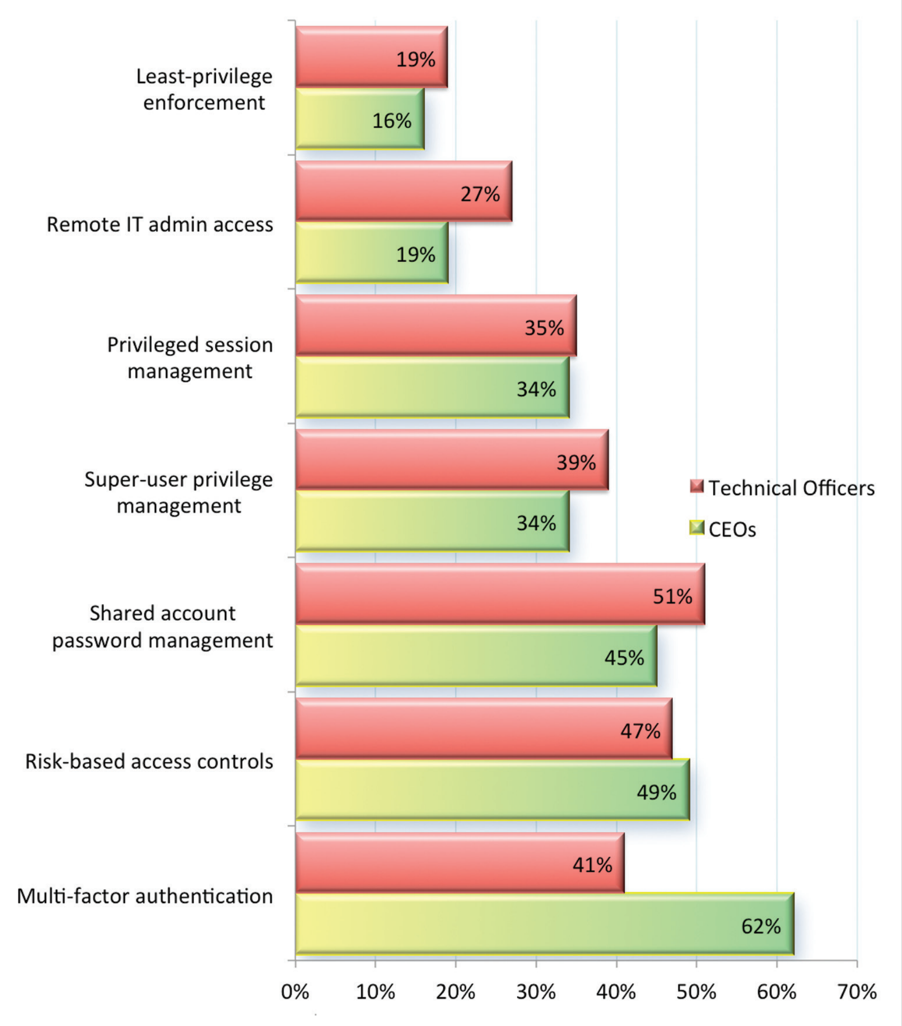
“We’re moving towards a situation where people have no access to anything unless they need it. That’s kind of the nirvana state”

Scott points to machine learning systems that can learn users’ habits. If, for example, an employee routinely logs in with known devices from a specific location in Paris at regular times of the day, then you might need to do very little authentication at all. However, if that same user logs in 20 minutes later from Nice then an intelligent system is going to spot that and immediately initiate an authentication process, possibly involving two-factor authentication, such as sending a PIN code to the user’s registered smartphone.

Access errors

Pretty much by definition, a data breach is when someone is able to get unauthorised access to information. Identity and access management (IAM) is one of the pillars of information security and a fundamental tool in managing the famous CIA security triad – confidentiality, integrity and assurance. So what’s going wrong?

“It’s really too much privilege, too much access to too many things,” says Scott. “We’re moving towards a situation where people have no access to anything unless they need it. That’s kind of the nirvana state. There’s also the fact that passwords are plainly past their sell-by date.”



Which aspects of identity management are perceived as the most difficult to manage. Source: Dow Jones Customer Intelligence/Centrify.

Policies and processes can only go so far in ensuring that users access only the things they’re meant to. Scott insists that there has to be something to back this up – a technological solution to enforce the rules.

“One of the things about zero trust that people will sometimes says is, ‘Oh, you mean I don’t trust my employees?' It’s not about whether you trust them as individuals”

“As time goes on, we’re seeing that it’s not just about people accessing certain applications, or admins accessing systems,” he says. The real picture is far more complex, including an increasing amount of machine-to-machine communication and – critically – widespread use of software as a service (SaaS) solutions. That complicates the management of privileges considerably because now you’re having to deal with things like privilege management through, say, the AWS console. This can lead to access management being fragmented – perhaps based around Active Directory for the corporate network but with each cloud-based service requiring you to use its own console.

“It’s been piecemeal,” says Scott, “and the breaches are happening in the gaps between these solutions. The ability to have one central solution is very attractive.”

Getting in the way

Even with centralised solutions available, some people (although perhaps not those with genuine security experience) can still recoil from the idea of least privilege because they suspect that it will get in the way. No system works with 100% efficiency and one day, they suspect, they'll be prevented from logging on to a system or accessing some information they need because of a slight misconfiguration or over-zealous settings.

"It's a reasonable position to come from, but the alternative is giving people access to everything," insists Scott. "One of the things about zero trust that people will sometimes say is: 'Oh, you mean I don't trust my employees?' It's not about whether you trust them as individuals; the danger is, what if somebody is masquerading as one of those trusted people? It might not be the fault of that individual at all."

Zero trust linked to a machine learning-based approach driving user authentication will help to overcome many of these fears by making authentication easier, Scott believes. That's the carrot and those nasty headlines about breaches, which just seem to keep on coming, provide the stick.

"The desire to not risk a breach is beginning to outweigh the possible mistrust in security solutions," says Scott.

Identity maturity

In many organisations, identity and authentication are a mess. Users are having to manage multiple sets of credentials – for the network, for specific applications on the network, for SaaS applications and on and on. You might have a dozen passwords to remember, a SecureID keyfob to carry and two-factor authentication PINs arriving on your smartphone.

From the IT department's point of view it must sometimes feel as though it would be easier to rip and replace – start from scratch with one authentication system for everything.

"Nobody really is in a position to be able to do that," says Scott. What they can do, however, he says, is implement solutions that integrate all those systems under one management umbrella.

"When somebody leaves the company, if they've got these 15 different accounts in 15 different places, realistically are you ever going to de-provision them properly?"

"It's a situation that's got to improve," he says. "So one of the first things you can do to improve your identity maturity, if we can call it that, is – if you're, say, a company that uses Active Directory – let's use that as the single source of truth. Of course, it's not always going to be Active Directory. We're seeing more and more companies that don't have any on-premise infrastructure at all. They use Google Directory, AWS or Google Compute or whatever. And these are all good place to start in consolidating identity."

Once you've got that core authentication service sorted, you can add functionality such as two-factor authentication, verifying devices and any new capabilities that emerge as technology develops. Indeed, it's possible that people are currently underusing the technology they already have, such as Active Directory.

"If they're getting into a situation where they have different user names for lots of different SaaS applications, for instance, then yes, they're underusing that single directory as a source of truth," says Scott.

"There are lots of different methods of authentication around now and I need to use my password less and less, which in turn means I can make it more complicated"

He adds: "Also, when somebody leaves the company, if they've got these 15 different accounts in 15 different places, realistically are you ever going to de-provision them properly? If you were using Active Directory effectively, all you've got to do is disable that Active Directory account and all the access has gone. When I'm talking to a roomful of people, there's always going to be a percentage of people in there who've left their company in the past six months and still have access to those systems – and that's really a breach waiting to happen."

Leaving passwords behind

So are we ever going to get rid of passwords?

Continued on page 20...

...Continued from page 19

"It's going to be a long time," reckons Scott. "We're moving away from them slowly. There are lots of different methods of authentication around now and I need to use my password less and less, which in turn means I can make it more complicated, or I can make it a pass phrase. But there are still a lot of passwords out there, and there are still a lot of people who've got 'password' as their password. So we really need to do everything we can to help them sort themselves out."

Those kind of issues don't necessarily need a technological solution. Proper password practice is something organisations can – and should – address through policy and training. The latter is also hugely important in dealing with threats such as phishing.

"We're all going to click on a bad link one of these days," says Scott. "It's just a matter of time. Whether we then enter our password on a dodgy website is within the lap of the gods. So that's why we need this zero trust approach – to make sure that if our credentials are stolen, the system will protect itself against attack."

> ***"We really need to be making sure that we're addressing privileged access. It's all about reducing the attack surface"***

This brings us back to the Verizon figure of 81% of breaches involving weak or stolen credentials. In terms of the overall threat landscape, what part does the problem of stolen or leaked credentials play?

"It's a huge part of it," says Scott. "We really need to be making sure that we're addressing privileged access. It's all about reducing the attack surface. If you get hit by ransomware, it becomes a big, big problem if you are a privileged user, or if a privileged user's credentials are stolen. So it all comes back to identity and only having appropriate access."

On the same page

It would help, then, if both business executives and senior IT staff were on the same page when it comes to dealing with this threat. So why aren't they?

"It's difficult to say," says Scott. "The CEOs are on a learning curve. There's more visibility now in the C-suite – of breaches and suchlike. So it's a question of time. And, of course, these aren't IT people, so they're being influenced to a certain extent by the high-profile issues – WannaCry, the NHS attacks, all those things. The CIO or CTO would understand that there's a bit more to it than that. Everyone needs to speak in each other's language as well. It's beholden on the CTO, CISO and all of those people to talk in the language that the CEO will understand, which is all about risk, about cost to the business. It's got to be put in CEO speak."

This is also important when it's the CEO who gets the final say in where money gets spent on security. "If they're holding the purse strings," says Scott, "that's where the disconnect needs to be addressed. They need to be given the right reasons to spend money on the right things."

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Computer Fraud & Security *and its sister publication* Network Security.

References

1. 'CEO Disconnect is Weakening Cyber Security'. Centrify. Accessed Mar 2018. www.centrify.com/resources/ceo-disconnect-weakening-cyber-security/.
2. Cyber Essentials, homepage, Accessed Mar 2018. www.cyberessentials.ncsc.gov.uk/.
3. '2017 Data Breach Investigations Report'. Verizon, 2017. Accessed March 2018. www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

EVENTS

2–3 May 2018
InfoSecurity Denmark
Copenhagen, Denmark
www.infosecurity.dk

14–20 May 2018
NorthSec
Montréal, Canada
www.nsec.io

17–8 May 2018
RuhrSec
Bochum, Germany
www.ruhrsec.de

29 May – 1 June 2018
CyCon: International Conference on Cyber Conflict
Tallinn, Estonia
https://ccdcoe.org/cycon/

1–2 June 2018
WarCon
Warsaw, Poland
http://warcon.pl/

5–7 June 2018
InfoSecurity Europe
London, UK
www.infosecurityeurope.com

25–29 June 2018
Hack in Paris
Paris, France
https://hackinparis.com

30 June – 1 July 2018
Nuit du Hack
Paris, France
www.nuitduhack.com/en/

2–6 July 2018
OWASP AppSec EU
London, UK
https://2018.appsec.eu/

19 July – 23 August 2018
IEEE Cyber 2018
Tianjin, China
http://ieee-cyber.org/2018/