ELSEVIER

network SECURITY

ISSN 1353-4858 June 2016

www.networksecuritynewsletter.com

Featured in this issue:

What the GDPR means for businesses

The long-awaited General Data Protection Regulation (GDPR) of the EU is nearly upon us, and every organisation that does business in, or with, the EU will have to comply with it.

The GDPR expands the scope of data protection so that it applies to anyone or any organisation that collects and processes information related to EU citizens, no matter where they are based or where the data is stored. Colin Tankard of Digital Pathways examines what effect the new regulation is likely to have on organisations.

Full story on page 5…

Why people are key to cyber-security

As organisations have become increasingly dependent on technology, the opportunities for thieves have grown.

Experienced thieves with a plan of action in place will always locate and maliciously target the greatest source of weakness – people. But by properly engaging the people in your organisation in the battle against attackers, you can turn your biggest weakness into your greatest asset, argues Mark Hall of Redcentric.

Full story on page 9…

The battle for privacy

Privacy in the digital realm has been an issue bubbling away for decades, pretty much since we've been communicating with computers.

Now, it seems, significant battle lines are being drawn – not between the public and the authorities, as one might expect, but between government intelligence and law enforcement agencies and technology companies. In this interview, Javvad Malik of AlienVault discusses the recent Apple/FBI controversy and the ethical issues it raises for the tech industry. And he explains how we as technology users have an important role to play in keeping ourselves safe online.

Full story on page 11…

Millions of user credentials for popular sites sold on dark markets

Databases containing user credentials for a number of major sites have suddenly become available on underground cyber-crime forums and dark markets, even though the breaches that led to the data leaks are years old in many cases.

Back in 2012, LinkedIn suffered a breach, as a result of which 6.5 million account details turned up on a Russian forum. Now it appears the leak was much worse than first admitted. Security researcher Troy Hunt says that a database of 167 million accounts is being

Continued on page 2…

Contents

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

Publishing Director: Bethan Keall

Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Senior Editor: Sarah Gordon

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

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Prices:
€1424 for all European countries & Iran
US$1594 for all countries except Europe and Japan
¥189 000 for Japan
Subscriptions run for 12 months, from the date payment is received.
More information:
http://store.elsevier.com/product.jsp?isbn=13534858

12987

Pre-press/Printed by
Mayfield Press (Oxford) Limited

…Continued from front page

offered for sale on underground markets by someone going by the name 'Peace'. This haul comprises 117 million account details that include email addresses and SHA-1 hashed passwords, many of which have already been cracked because of LinkedIn's failure to use a salt.

Many of the passwords will be obsolete now because LinkedIn encouraged people to change them in 2012. However, a number of users have confirmed that some of the passwords in the database are current. Indeed, Facebook CEO Mark Zuckerberg has had his Twitter and Pinterest accounts hijacked, with the hackers claiming Zuckerberg had used the password 'dadada' in the breached LinkedIn database. According to some sources, Zuckerberg is known for his habit of recycling passwords. He's not the only person who is poor at managing passwords, though: the leaked database shows many people using the inevitable '123456', 'linkedin' and 'password'.

Not long after the breach was discovered, it was announced that Microsoft had agreed to buy LinkedIn.

Hunt also said that millions of IDs from adult dating site Fling, which was breached in 2011, had also been put up for sale.

Just over 360 million MySpace account records have been offered on the dark web, too – again by 'Peace'. These had hashed passwords, but many had been cracked. For its part, MySpace suggested that the accounts related to the older version of its platform, before a switch in June 2013. No breach was reported at that time and it's unclear whether MySpace simply didn't know about it or failed to report it. It has invalidated all passwords in use up to that time.

A leak of Tumblr IDs also seems to date from a breach in 2013, but which wasn't disclosed by the Yahoo-owned company until May 2016. The database is being offered by the same hacker who is selling the LinkedIn database. In this case, the 65 million account details seem to have properly salted hashes of the passwords. However, the email addresses in the database could be useful to spammers and phishers.

And the records from yet another 2013 breach, this time of the now-defunct iMesh site, are also for sale. In this case, 51 million records are up for grabs, and they include usernames, passwords, email addresses and location. The passwords were hashed using the now-deprecated MD5 algorithm, with no salt.

A database of just under 33 million Twitter credentials is also up for sale, although Twitter itself says it hasn't been breached. It's possible this database has been created by trying passwords from other breaches.

"We have very strong evidence that Twitter was not hacked, rather the consumer was," said LeakedSource, which discovered the database being offered for sale on underground forums. "These credentials however are real and valid. Out of 15 users we asked, all 15 verified their passwords."

The FBI has issued a warning saying that criminals are attempting to cash in on these breaches via blackmail threats. The criminals contact victims of the data breaches and claim to have hacked into their accounts using the leaked credentials. They then threaten to reveal the victim's secrets unless they receive 2 bitcoins.

"If you believe you have been a victim of this scam, you should reach out to your local FBI field office, and file a complaint with the IC3 at www.ic3.gov," the FBI said in a statement. "Please include the keyword 'Extortion Email Scheme' in your complaint, and provide any relevant information in your complaint, including the extortion email with header information and Bitcoin address if available." There's more information here: http://1.usa.gov/236RhLF.

A large number of users of the TeamViewer collaboration and remote connection platform have complained that their accounts have been accessed, and that PayPal and bank accounts have been drained by criminals. For its part, TeamViewer insists there has been no breach of its systems. Instead, it claims that its customers have had their accounts accessed as a result of account breaches elsewhere – such as LinkedIn – and because the customers have re-used the same passwords. It has also said that too many customers are using weak passwords. However, there are users who say that their accounts were accessed even though they use unique passwords and/or two-factor authentication.

In brief

FBI fails to get warrantless browser access

An attempt to give the FBI warrantless access to people's browser histories has been thwarted by US politicians. However, in the process, a group of amendments that would have made access to private information more difficult has also been put on hold. A bipartisan group had pushed through the ECPA Amendments Act, which had passed through the House and was close to becoming law. It would have made changes to the 1986 Electronic Communications Privacy Act which currently allows law enforcement agencies to gain access to any email that has been read or is more than 180 days old. The amendments would, among other things, have eliminated the 180-day proviso and would have required law enforcement officers to obtain warrants. However, a further amendment added at a late stage by Republican Senator John Cornyn from Texas would have given the FBI warrantless access to individual's browser histories – all the agency would require is a more easily obtained National Security Letter, which the agency can issue itself. In order to avoid creating this new power for the FBI – described as a "poison pill" – the sponsors of the ECPA Amendments Act have put the Bill on hold.

North Korea attacks thousands of computers

More than 140,000 computers owned by 160 South Korean organisations have come under attack by North Korea. According to the Government in Seoul, the targeted firms were all connected with the defence industry, and 40,000 defence-related documents and files were stolen, along with 2,000 others. According to Seoul's cyber investigation unit, these included plans for the wings of the F-15 fighter jet. The IPs of the attacking systems were the same as those used in previous mass attacks on South Korea. The North Korean Government has denied responsibility for the attack.

Pentagon hacked; bugs found

An invitation to 'Hack the Pentagon' resulted in the discovery of more than 100 vulnerabilities in the organisation's systems. Around 1,400 penetration testers took part in the bug bounty scheme which paid out prizes of up to $14,000 for each bug found. Participants had to register and agree to a background security check before being allowed to attack the Pentagon's systems. US Defence Secretary Ashton Carter told the Defense One conference in Washington that the scheme had significantly reduced the cost of vulnerability discovery. "They are helping us to be more secure at a fraction of the cost," he said.

Symantec acquires Blue Coat

The acquisition of Blue Coat by Symantec has raised some concerns in the security industry. Recently, Blue Coat was found to be using an SSL certificate that allowed security devices to masquerade as legitimate hosts. The certificate was signed by Symantec using its position as a root certificate authority. Among its many networking products, Blue Coat produces systems that are designed to monitor traffic on networks to look for suspicious activity. It's common, for example, for organisations to deploy deep packet inspection (DPI) devices that effectively act as a 'man in the middle', decrypting SSL traffic from users before re-encrypting to pass it on to its destination – and vice versa. However, usually these devices use an organisation's own certificates which must be manually accepted by the end users. But the certificate recently used by Blue Coat had root authority, meaning it would be accepted automatically by any browser with the user not knowing that the traffic had been intercepted. Blue Coat said the certificate was only ever used for internal testing. However, the merger of one company that specialises in such interception (and which has a track record of sales to countries with poor human rights records) with another capable of issuing root level certificates has left some people uneasy.

User error

Two-thirds of data breaches in the UK in the first three months of 2016 were caused by human error, according the results of a Freedom of Information request. Some 62% of breaches reported to the Information Commissioner's Office (ICO) were the result of mistakes made by staff, whereas the more high-profile breaches resulting from insecure websites and hacking accounted for only 9%. However, these figures are for numbers of breaches rather the number of records compromised. A large proportion of the errors uncovered by Egress Software Technologies in its Freedom of Information request consisted of data posted or faxed to the wrong recipient, loss and theft of paperwork and data emailed to the wrong recipient. The courts and justice sector has experienced a six-fold increase in reported data breaches over a three-year period. Other organisations that have experienced a growth in breach incidents are insurance firms (317%) and charities (109%).

DNS puts businesses at risk

A failure to secure DNS is costing UK businesses as much as £1m a year each, claims networking firm EfficientIP. A quarter of firms aren't implementing any kind of security at all, and three-quarters of them have been victims of DNS attacks. While the majority (79%) of organisations are aware of the risks associated with DNS, only 59% were using any form of DNS security. The research also revealed that the most common attack types, which businesses claim to be aware of, are also the main causes of business outages and data theft. The DNS attacks that have the largest impact on an organisation include: DDoS attacks, with 22% of the companies surveyed having been subject to DNS-based DDoS attacks in the past year; data exfiltration, with 12% of organisations in North America and 39% in Asia having had data exfiltrated via DNS in the past year; and zero-day vulnerabilities, affecting almost 20% of the businesses surveyed. Less than 23% of those surveyed recognised zero-day attacks or DNS tunnelling as risks; only 29% were aware of cache poisoning; and only 30% were aware of DDoS attacks. While firewalls can protect on a basic level, they're not designed to deal with high-bandwidth DDoS attacks, or detect DNS tunnelling attempts (the majority of DDoS attacks are now over 1Gbps).

New security rules across the EU

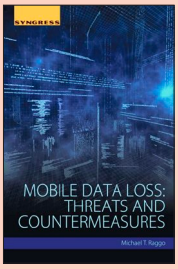
New rules have come into force across the EU in an effort to make the networks and information services of key industries more secure. The European Council has published the Network and Information Security (NIS) directive which requires organisations that provide essential services, such as energy, transport, health and finance, as well as 'digital service providers', including online marketplaces, search engines and cloud services, to implement certain basic risk reduction practices. It also imposes a requirement for them to report major security incidents. It's left for member states to decide which organisations fit into the category of essential service providers, as these face the strictest rules. Digital service providers will be subject to less-strict regulations and small companies will be exempt. The rules also lay out procedures for security cooperation between EU member states, which must have the rules fully in place and operating by the middle of 2019. There's more information here: www.consilium.europa.eu/en/policies/cyber-security/.

Ransomware strikes university

As cyber-criminals continue to shift their focus of attack from individuals to enterprises, another organisation has fallen victim to ransomware. The University of Calgary, Canada paid out CDN$20,000 after an email server was infected. As many as 100 systems may have been affected in total. Unusually, the University believes that the malware was deliberately planted by an outsider, rather than the usual exploit vector of an employee falling for a phishing scam. It appears the University did not have adequate back-ups that would have allowed it to recover from the attack without paying the ransom.

Reviews

BOOK REVIEW



Mobile Data Loss: Threats and Countermeasures

Michael Raggo. Published by Syngress. ISBN: 978-0-12-802864-3.
Price: 21.95, 55pgs,
e-book and print editions available.

While the focus of many organisations has been on protecting their servers and network infrastructure, a rapid evolution has been underway at the endpoints of their networks. The changes wrought there may have rendered what little attention they have given to the endpoint largely null and void.

For decades, the device with which the user interacted was a PC sitting on the desk. It didn't move, it was owned by the organisation and was (fairly) easily configured, standardised and maintained. You, as an IT department, knew what software was running on it because you'd put it there yourself, usually in the form of a standardised image. You could roll out patches in an orderly fashion and all the data that flowed to and from the machine went through your network and the protective mechanisms you'd put in place.

Not any more. The users' devices are as likely to be in their pockets as on their desks. They may be running operating systems you don't officially support and apps over which you have no control. Both hardware and software are likely to be a user's personal property. And yet that device is still logging on to your internal networks, well behind your firewalls and intrusion detection systems, while maintaining connections to the Internet over mobile networks that completely bypass your defences.

To make matters worse, the user is probably keeping some of your organisation's sensitive information – emails and files – on a device that is easily lost or stolen. This phenomenon of Bring Your Own Device (BYOD), or 'shadow IT', has proven to be unstoppable. Even those organisations that try to nip it in the bud by issuing staff with mobile devices soon find that employees will use these for personal activities – the so-called Corporate Owned, Personally Enabled (COPE) phenomenon – which still leaves the company open to the risk of vulnerable devices on their networks.

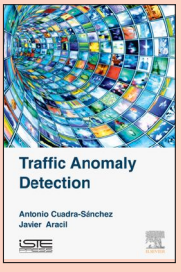
It isn't all doom and gloom, though. As this short book explains, Enterprise Mobile Management (EMM) (also known as Mobile Device Management, MDM) solutions give back a large degree of control to the organisation, even when personal devices are involved, so long as the right systems, processes and policies are in place. Critically, IT departments must be careful not to lock down the devices too tightly. The reason that users employ mobile devices in the first place is because of the flexibility and freedom they provide: if your mobile policies and deployments infringe on that and make the devices difficult to use, your staff will simply find ways around the system.

This book offers a high-level view of how your organisation can reap the benefits of mobile devices – such as improved productivity – while minimising the risks. You can read it partly as a strategy document and partly as an implementation blueprint. It lays out the major risks that these devices introduce into the corporate network and how you address them with a carefully designed and implemented MDM solution. And it also touches on how all this fits into your compliance posture, especially relating to PCI and HIPAA. At around 55 pages, it's not exhaustive. But if you're just starting to address these issues, then this book concisely and clearly lays out the issues you need to face and the overall strategies for doing that.

There's more information here: http://bit.ly/1ttIpUx.

– SM-D

BOOK REVIEW



Traffic Anomaly Detection

Antonio Cuadra-Sánchez and Javier Aracil. Published by Iste Press. ISBN: 978-1-78548-012-6.
Price: 57.95, 72pgs, paperback.

It seems an obvious statement, but the traffic you don't want on your networks – the malicious traffic from malware and intruders – simply shouldn't be there. It's traffic that doesn't form part of the normal picture of the normal, day-to-day activity. You'd think, then, that it would be easy to spot – assuming that you're looking in the right places.

It's tricky, though. Modern networks are complex environments. Traffic ebbs and flows during the day, varies from day to day and season to season, and is subject to sudden spikes and lulls, sometimes brought on by factors that are unforeseeable, sometimes invisible and often outside your control.

Many of our defence mechanisms are relatively crude. The classic 'port and protocol' firewall, for example, has long been rendered ineffective by encryption and the continuing trend towards pushing so much traffic through web protocols. Intrusion detection systems attempt to add a little more intelligence, but in the end it all comes down to understanding what constitutes legitimate traffic for your specific environment and what deserves closer scrutiny as possible malicious activity

In this book, the authors don't attempt to present a practical solution to this issue – rather, their focus is on the theoretical aspects of determining anomalous traffic. Their approach is based on analysing multimedia traffic across a network. Most corporate networks today carry a mix of traffic types leading to a complex pattern of protocols and packet volumes, so this is a good choice in terms of dealing with the current challenges of spotting unusual behaviour.

The book begins by analysing the algorithms typically used for detecting sudden changes in regular processes. It makes use of statistical control charts (SCCs) that show divergence from the norm through the use of standard deviation analysis. But as the authors point out, no one SCC is capable of working in all cases because so much depends on the nature of the underlying traffic. So a 'cumulative sum' approach is used to detect changes. The book then goes on to study how you pick the right time period from which to draw your data before aggregating it. It then reviews and compares various detection methods before finally proposing information theory-based technique.

This is all highly theoretical work and it remains for someone to implement the ideas in a form that you can use as part of your security activities. But it's bound to be of interest to those developing security solutions.

There is more information available here: http://bit.ly/1UN1Rns.

What the GDPR means for businesses

Colin Tankard

Colin Tankard, Digital Pathways

The long-awaited General Data Protection Regulation (GDPR) of the EU was provisionally agreed in December 2015.[1] The final details are still being ironed out, but publication of the final version of the regulation is expected around July 2016.[2] There will then be a two-year waiting period until every organisation that does business in, or with, the EU must comply with the regulation. Since it is a regulation, not a directive, compliance is mandatory, without the need for each member state to ratify it into its own legislation.

Previous data protection legislation had become fragmented across the EU as different countries added to the basic principles enshrined in the original directive of 1995. Some countries added clauses to require breach notification and sanctions currently vary widely. Some countries, such as Spain, fine heavily and often: others, such as France, hardly mete out any fines at all. This has resulted in the situation where organisations doing business across the region face a legal minefield of differing interpretations of data protection.

Another reason why new legislation was needed is that the original directive of 1995 was formulated in what now appears to be a different technological era. Back then, just 1% of the world's population was using the Internet, but today it is almost ubiquitous across the EU. Cloud computing and social media were not known then, nor were smartphones or tablets. Today, the vast majority of information is produced and consumed electronically, making it harder to protect.

The major changes

The GDPR expands the scope of data protection so that anyone or any organisation that collects and processes information related to EU citizens must comply with it, no matter where they are based or where the data is stored. Cloud storage is no exception.

The definition of personal data has also been expanded. It states that personal data includes information from which a person could be identified, either directly or indirectly. Under the new definition, identifiers such as IP addresses and cookies are included as personal information.

Prior to the GDPR, there has been no uniform legislation regarding breach notification, except for electronic communications service providers under the ePrivacy directive. Some countries added provisions to their legislation to cover breach notification, but not all. The GDPR introduces mandatory breach notification unless the breach is unlikely to result in a risk to the rights and freedoms of the data subjects concerned. A particularly onerous demand in the new regulation is that organisations suffering a data breach must notify data protection authorities within 72 hours of its discovery.

"A particularly onerous demand in the new regulation is that organisations suffering a data breach must notify data protection authorities within 72 hours of its discovery"

Sanctions for non-compliance with the regulation have not only been made uniform, but they have been increased considerably. For a minor breach, organisations can be fined up to 2% of their worldwide revenue or 10 million euros, whichever is higher, although a warning can be given for first offences. For more serious violations, fines of up to 4% of worldwide revenues can be imposed or 20 million euros, whichever is higher.

Organisations with substantial data processing activities are required to appoint a data protection officer, who must function independently of the business. However, one such officer can be shared among organisations.

"Under the GDPR, notification is only required in the member state deemed to be the headquarters of the data controller or processor, or where most of the processing takes place. This will reduce the costs and efforts of compliance for organisations"

Data impact assessments will also be required where processing of data is deemed to be high risk for the rights and freedoms of the data subjects involved. Such an assessment must detail the safeguards, security measures and mechanisms that are in place for addressing risk and ensuring compliance. Both of these demands will raise the cost of complying with the regulation for organisations.

Individual rights

Another area that will make compliance harder is that the rights of individual data subjects are being expanded. They must unambiguously give their consent for their data to be processed, which must be informed and voluntary; have the right to access information held on them; and may object to the processing of their data where there are legitimate grounds for doing so. One new requirement, which has been perceived as controversial by some, is that the right to be forgotten has been solidified, requiring data controllers and processors to remove data that is

considered to be inadequate, irrelevant or no longer relevant. This will require that organisations know exactly what information they hold and where it is stored.

However, one thing that will make it easier for data controllers and processors is the introduction of the one-stop-shop concept. Previously, it was necessary to notify the data protection authorities in each EU member state before processing could begin, which was a time-consuming and often costly process. Under the GDPR, notification is only required in the member state deemed to be the headquarters of the data controller or processor, or where most of the processing takes place. This will reduce the costs and efforts of compliance for organisations.

Data transfers are still prohibited to jurisdictions deemed to have inadequate levels of security, unless authorised by a supervisory authority. This requires the negotiation of contracts for the data transfer. Binding corporate rules, standard data protection clauses adopted by the European Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority may all be used for enabling the international transfer of data. Of these, binding corporate rules are considered to be the gold standard for data transfer. EU model clauses remain valid.

"According to Ovum, 52% of organisations believe that the GDPR will result in fines for their business and 68% feel that it will dramatically increase the costs of doing business in Europe"

However, the Safe Harbour Agreement that was negotiated with the US has been deemed invalid and may no longer be used owing to fears that it was enabling bulk surveillance by authorities. A new agreement has now been reached in the form of a Privacy Shield Agreement, which creates multiple enforcement mechanisms for data protection authorities, as well as multiple paths for remedies for EU citizens. Although not all the details are yet known, it is expected that requirements for consent, as well as for securing data, will be higher.

Time to get your house in order

Many are worried about the impact of the GDPR. According to Ovum, 52% of organisations believe that the GDPR will result in fines for their business and 68% feel that it will dramatically increase the costs of doing business in Europe, with some believing that their budgets will need to increase by some 10% to deal with its ramifications over the next two years.

Two years may seem a fair amount of time to prepare, but it will pass quickly. The time to start preparing is now. Polls conducted during a recent webinar sponsored by Vormetric found that 48% of attendees are already preparing for the GDPR, but 30% did not know whether they were or not. This is despite 91% stating that they were at the very least worried about non-compliance.

What is required for compliance

As with the 1995 directive – and, indeed, many directives and regulations – the GDPR is not prescriptive in the technologies that should be used to achieve compliance. This is nothing out of the ordinary, since any legislation that is too prescriptive runs the risk of quickly becoming obsolete, especially given the rapid pace of technological change in today's world.

Rather, the GDPR states that organisations need to implement appropriate technological and operational safeguards for securing data, including putting in place strong privacy controls. It states that organisations should adopt internal measures that meet the principles of data protection by design and default. What this means in practice is that data protection and privacy must be considered right from the beginning of the security planning process.

"Organisations should adopt internal measures that meet the principles of data protection. Data protection and privacy must be considered right from the beginning of the security planning process"

There is, however, one exception to the regulation being non-prescriptive in terms of technologies. Encryption is specifically called out, along with pseudonymisation, as an appropriate safeguard for securing data. If they encrypt data, organisations that suffer a data breach are not obligated to notify data subjects as the data is considered to be adequately protected, as long as the encryption was properly implemented.

Keeping pseudonymous data separate

Where pseudonymisation is used, in which data is processed in such a way that it cannot be attributed to a specific individual, pseudonymised data must be held separately from any additional information stored in clear form to ensure

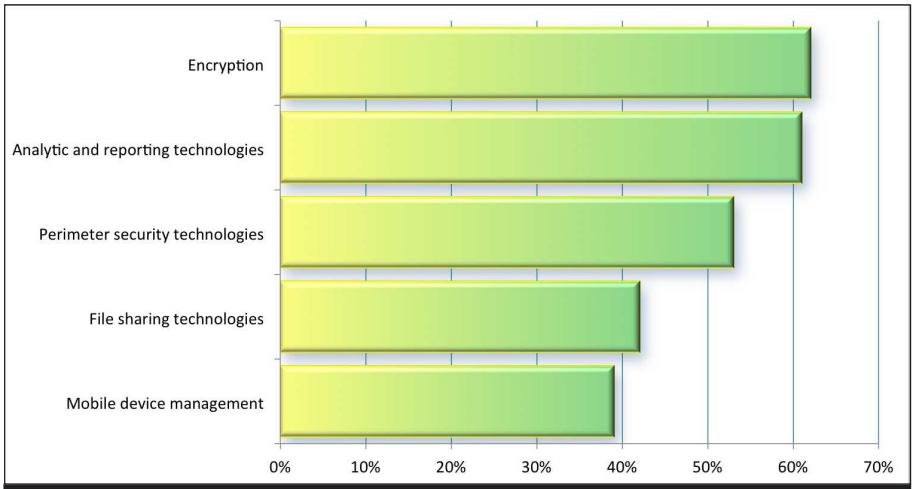


Figure 1: Technology investments for achieving data protection regulation compliance.

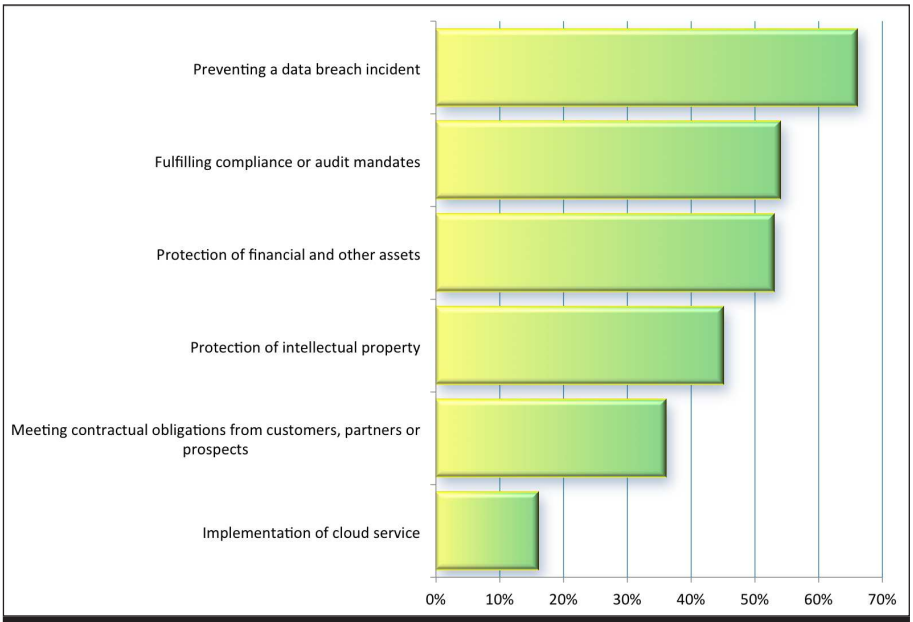


Figure 2: Primary drivers for encrypting data.

that it cannot be attributed to a specific individual. As Figure 1 shows, encryption is considered to be the top technology control for data protection.

A separate survey looked to gauge what the primary drivers for encrypting data are, as shown in Figure 2.

Law firm Baker & McKenzie states that there are five initial steps to make before considering measures to take to achieve compliance. These are:

- Assess whether or not you will fall within the scope of the GDPR.
- Understand the new compliance obligations, decide how to comply with them and assess their operational impact.
- Identify new responsibilities and risks and consider how to address those risks.
- Understand the market, in particular what data controllers will require from processors moving forward and what your competitors will be willing/not willing to agree to vis-à-vis data controllers.
- Devise a strategy for negotiating processing agreements.

Technology controls

As stated above, encryption is specifically called out in the GDPR and should be the default option for protecting all data, both when data is being transmitted and is in storage. This includes both structured and unstructured data stored in databases, or included in spreadsheets, word documents, presentations, emails and archives. Even when data is stored in the cloud or on endpoints, cryptographic keys should be kept with the organisation responsible for collecting or processing the data to prevent the opportunity for inappropriate access by third parties, which could lead to charges that the encryption was not adequately implemented. Strong security controls should also be applied within the organisation to ensure that only those entitled to can access keys.

"Should data be put to uses other than those to which the data subject gave his or her consent, the data subject may seek redress in the form of compensation"

Even though data is being encrypted, it is still good practice to minimise the amount of data collected. This will not only help to reduce the burden of protecting massive datasets, but will also mean that the organisation is less likely to fall foul of requirements in the GDPR that data only be used for purposes for which it was collected, and no other. Should data be put to uses other than those to which the data subject gave his or her consent, the data subject may seek redress in the form of compensation.

While encryption is an extremely good tool for data protection, it is not sufficient by itself. Organisations should ensure that they have adequate access controls in place to prevent unauthorised access when the data is decrypted and to control what users can do with the data according to their role. For example, a systems administrator needs to be able to perform management tasks such as back ups but should not be able to read the content of the data – eg, in an HR system the server operation team need to be able to take care of the system and know that data is there but should not be able to read the contracts of employment. This applies, in exactly the same way, for applications accessing data, which should have access controls applied to them.

"All security systems should be continuously monitored, taking into account all the risks associated with data processing and storage, including inadvertent loss or destruction"

For this reason, the controls should be tied to back-end databases such as Active Directory, which will help in defining granular entitlements and ensuring that they are kept up to date as things change, such as a person being promoted or moved to another role.

Where organisations find the management of Active Directory very complex there are tools available, such as those from 8Man, that enable a business to have a graphical view of user rights and easily remove or add controls to ease the burden of user management. Furthermore, linking the authentication of users or applications to the encryption enhances the controls available within Active Directory and provides a fine grain audit trail of user access to data that further benefits the ability to monitor and track the 'insider threat' that faces many organisations.

Entitlement to data

The use of strong authentication will help to ensure that the people accessing data are who they say they are so that a user with entitlements to access data cannot pass those entitlements on to someone else.

In order to test, assess and evaluate that

controls are effective and to ensure that they are working at all times, all security systems should be continuously monitored, taking into account all the risks associated with data processing and storage, including inadvertent loss or destruction. Integration with security information and event management systems will provide visibility over events occurring over the network, which can be analysed to ensure that security and compliance objectives are being met. This will also provide the audit trail that is required to prove that controls are working properly.

Industry standards and best practice frameworks

The use of industry standards and best practice frameworks can help organisations to manage the risks that they face while adding greater efficiency and sustainability to their operations. They enable best practices to be embedded into an organisation.

The CIS critical security controls, which are listed in Table 1, can be considered to be a checklist of the controls that organisations should have in place to ensure that their security posture is up to the task of managing risk. These controls are a recommended set of actions that will provide organisations with specific and actionable ways to boost their cyber-security capabilities, allowing organisations to prioritise actions should an attack occur in order to achieve the best results with the least effort.

"The time and effort required to achieve compliance will vary greatly from one organisation to another, but it is well worth the effort"

Security standards such as ISO 27001 and ISO 27002 will help organisations to ensure that they have in place effective information security programmes. ISO 27001 was originally created with the intention of helping to manage the security of government services and citizen data in the hands of service providers. The use of ISO 27001 will help to ensure the principle enshrined in the GDPR that appropriate technological and organisational measures are in place to protect information. It will help organisations to define responsibilities, such as who is responsible for certain information assets and who can authorise access to data. ISO 27001 provides independent accreditation for information security management systems, while ISO 27002 is a code of practice that is not accredited by external parties. The use of either will help to show that an organisation has put in place strong controls should that organisation ever need to address issues related to negligence.

Control	Description
CSC 1	Inventory of authorised and unauthorised devices
CSC 2	Inventory of authorised and unauthorised software
CSC 3	Secure configurations for hardware and software on mobile devices, laptops, workstations and servers
CSC 4	Continuous vulnerability assessment and remediation
CSC 5	Controlled use of administrative privileges
CSC 6	Maintenance, monitoring and analysis of audit logs
CSC 7	Email and web browser protections
CSC 8	Malware defences
CSC 9	Limitation and control of network ports, protocols and services
CSC 10	Data recovery capability
CSC 11	Secure configurations for network devices such as firewalls, routers and switches
CSC 12	Boundary defence
CSC 13	Data protection
CSC 14	Controlled access based on the need to know
CSC 15	Wireless access control
CSC 16	Account monitoring and control
CSC 17	Security skills assessment and appropriate training to fill gaps
CSC 18	Application security software
CSC 19	Incident response and management
CSC 20	Penetration test and red team exercises

Table 1: SANS CIS critical security controls.

Conclusions

After years of wrangling, the GDPR is now a fact and compliance deadlines are looming. The time to start preparing is now. In fact, Digital Pathways has been promoting technologies that link access control to encryption for over 20 years. Organisations need to ensure that they are not caught out and face sanctions for non-compliance. With the right precautions in place, organisations should have little to fear. The time and effort required to achieve compliance will vary greatly from one organisation to another, but it is well worth the effort.

About the author

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

Resources

1. 'General Data Protection Regulation'. Wikipedia. Accessed May 2016. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation.
2. 'Regulation (EU) 2016/679 of the European Parliament and of the Council'. Europa. Accessed May 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

Why people are key to cyber-security

Mark Hall

Mark Hall, Redcentric

Cyber-security is one of the great issues of our time. As organisations have become increasingly dependent on computer and data communication technology, the opportunity for thieves has grown. Couple that with the lack of national boundaries in cyberspace and the relatively low probability of being caught and the risk/reward ratio makes cybercrime much more attractive than taking a sawn-off shotgun into a bank.

The 'attack surface' grows all the time. By 2020, it is estimated there will be 4 billion people online and the Internet of Things will be up and running, interconnecting 26 billion Internet-enabled devices and thereby allowing a thief who can find an entry point to jump from device to device.[1,2] After all, it only takes entry to one device for a cyber-criminal to gain access to every machine active on that server. Worryingly, there is also no sign of this growth of complexity ever stopping, so the opportunities for cyber-criminals will only increase. The same is true of the rewards cyber-criminals will gain for successfully hacking businesses, as the more data is stored digitally, the more valuable each hack will become.

"Most people have enough awareness to know they are exposed if they are not behind a firewall and most people have enough sense to run anti-virus software and keep it updated"

So it's unsurprising that organisations are improving their internal processes and are therefore getting better at protecting themselves. For example, software updates are usually implemented quickly or automatically now, so vulnerabilities are blocked before the attacker can exploit them. Vulnerabilities usually occur because different modules within a large software system are written by multiple coders, with differing habits. No matter how well specified and tested the modules are, there will always be slight variations in the way things work because each person does things slightly differently. It is these small differences the thief is looking for, as they can enable them to gain access to servers and networks that businesses believe are secure.

Firewalls are better than they were. Most people have enough awareness to know they are exposed if they are not behind a firewall and most people have enough sense to run anti-virus software and keep it updated across all of their devices, both at home and in the office. Simple attacks are therefore mostly blocked by technology. A reasonable guess is that 99% of attacks are blocked before they do any harm. However, that would still leave 1% of a large number that do get through. This may seem like a small figure but due to the interconnected world we live in, even a handful of successful hacks can put huge amounts of sensitive business and customer data in jeopardy. So, despite the clear improvements being made, it is clear that technology alone cannot defeat cyberthieves.

The weakness

Experienced thieves with a plan of action in place will always locate and maliciously target the greatest source of weakness – people. By nature, people are inconsistent and should therefore be a cause for concern for any business creating a cyber-security plan. After all, even the most secure of companies is only as strong as its weakest link. Some people care about protecting themselves online, while others do not realise the dangers that exist. Some are cautious about opening email attachments from unknown sources, but some are not and blindly open any email or attachment they receive, despite not knowing the sender. Unsurprisingly, these people often live to regret it. Their personal devices that they use for work could be compromised, sensitive data could be lost and the entire office could be put in danger – all thanks to erroneously opening one email.

"It's unsurprising there are rarely employee incentives for strong cyber-security, which is difficult to measure. After all, when done well, there are simply no attacks"

Thieves can and will exploit these inconsistencies and weaknesses for their own personal gain. However, more often than not, business policies do not help and instead can actually hinder the drive towards increased cyber-security. In the vast majority of business environments, the workforce's performance is gauged on easily measurable elements such as sales numbers, hitting deadlines and cost savings. In a world in which the C-suite is solely focused on business growth, goal-driven employees tend to favour these elements over anything else. It's therefore unsurprising that there are rarely employee incentives for strong cyber-security, which is much more difficult to measure. After all, when done well, there are simply no attacks and security can therefore be taken for granted.

Private lives

Outside the office, people are careless

online in ways they would never be in a more formal setting. Social networks create digital footprints that are often impossible to remove or improve once they exist – many people today know someone who has posted some images online that they regretted the morning after.

Unfortunately, many people don't realise the security implications that leading a lavish lifestyle of social media can have. It is not difficult for a researcher to move from reading personal information on Facebook to researching the same person on LinkedIn to find their professional profile, then to find their colleagues.

Worryingly, it can be this easy to find a way in, with hackers easily able to gain access to personal devices by emulating a colleague or claiming to be a friend who has lost access to their old social profile. Indeed, some people do this for a living, researching likely targets and finding all their personal details, before selling that profile, together with all the supporting information, on the dark web to criminals who will use it to steal from the person or their employer.

"It is not difficult for a researcher to move from reading personal information on Facebook to researching the same person on LinkedIn to find their professional profile, then to find their colleagues"

It's frightening how the theft of one person's identity can cause such a huge downward spiral – their financial information is in jeopardy of course, but the profiles of all their friends, loved ones and colleagues are also at risk. From a professional standpoint, the hacker will have access to the entire server and every member of the workforce with access to it. One successful hack can easily facilitate hundreds of resultant breaches.

Wasting time

So how should an organisation approach the soft, people issues involved in cyber-security? Perhaps the first recognition businesses should make is that people do not listen, do not pay attention and often simply do not do what they are told even when they do listen and understand. So businesses that spend days working on an in-depth cyber-security planning document and share it around their office so everyone is aware of exactly how to act online are likely wasting large portions of their time. There will always be a member of the team who just doesn't read it. The ability to influence and persuade is therefore much more important than the ability to write procedures. Unfortunately, the soft human resources and psychology skills needed to approach the issue in this way are often not the skills possessed by the people responsible for cyber-security.

"Businesses that spend days working on an in-depth cyber-security planning document and share it around their office so everyone is aware of exactly how to act online are likely wasting large portions of their time"

Cyber-security is generally seen as a part of the IT department. As such, it attracts IT professionals who understand and analyse issues before writing procedures to address them, but lack the necessary skills to train and persuade the professionals on the front line. Mandating does not work, but it is the way most organisations deal with the issue. However, those outside of the IT department often ignore technical issues, assuming they will be dealt with by the tech team. It is this attitude that cyber-thieves prey on as they know that the longer these values are the norm in the business world, the more successful their attempts will be.

Time to take a stand

As far as cyber-security is concerned, it often gets lost in the shuffle. Most organisations have poor management and auditing practices and weak or non-existent personal risk assessments and pre-employment screening. Simultaneously, communication between the arm of the business responsible for cyber-security and the workforce is almost non-existent. Many managers regard cyber-security as a nuisance they have to deal with, taking time away from what really matters in achieving their objectives.

It can be hard to generate a truly beneficial interaction between the people responsible for IT security and the rest of the organisation. People often do not like being told what to do, even when they listen.

"Many managers regard cyber-security as a nuisance they have to deal with, taking time away from what really matters in achieving their objectives"

Relationships take a long time to develop and need a lot of nurturing but employees will respond and contribute if they are treated like adults and persuaded to build a culture of online security awareness. The key is developing everyday practices that help people feel secure online and, over time, developing a culture in which people implement those practices without resentment and without thinking about them.

About the author

Mark Hall is director of public sector and security operations at Redcentric (www.redcentricplc.com), focusing on managed services and advanced software solutions for the public sector, including the National Health Service and UK Central Government. He also oversees the security strategy of Redcentric, ensuring that the company meets stringent compliance regulations to ensure data security for its customers.

Resources

- 'Linking Cyber-security Policy and Performance'. Microsoft. Accessed May 2016. www.microsoft.com/en-us/download/details.aspx?id=36523.

References

1. Callaham, John. 'Microsoft: Internet users will double to 4 billion worldwide by 2020'. Neowin, 11 Feb 2013. Accessed May 2016. www.neowin.net/news/microsoft-Internet-users-will-double-to-4-billion-worldwide-by-2020.
2. 'Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020'. Gartner, 12 Dec 2013. Accessed May 2016. www.gartner.com/newsroom/id/2636073.

The battle for privacy

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Network Security*

Privacy in the digital realm has been an issue bubbling away for decades, pretty much since we've been communicating with computers. Sometimes it has erupted into controversy, such as the public feud over encryption and the Clipper chip in the 1990s.[1] Now, however, it would seem that significant battle lines are being drawn – not between the public and the authorities, as one might expect, but between government agencies and technology companies. In this interview, Javvad Malik, security advocate at AlienVault, discusses the recent Apple/FBI controversy and the ethical issues it raises for the tech industry.

Access denied

Tensions between tech companies and the authorities have been evident for a while. The document leaks from former CIA and NSA contractor Edward Snowden first suggested some level of collaboration between US and UK intelligence agencies and firms such as Microsoft, Google and Facebook. But the companies themselves were quick to issue denials and some of them seem to be going out of their way to demonstrate independence – such as the use of so-called 'canary' clauses in their transparency reports (see Figure 2).

The event that led to a more direct clash between the two sides was the mass shooting in San Bernardino, California by Syed Farook and his wife Tashfeen Malik in December 2015.[2] They attacked fellow workers at the San Bernardino Department of Public Health, leaving 14 dead and 22 seriously injured. Quickly categorised – by both media and the authorities – as a terrorist attack, it was the deadliest such incident on US soil since the 9/11 atrocities of 2001.

One of the items left behind by Farook was a company-issued iPhone 5C. Naturally, the FBI wanted to carry out a forensic examination of the device but the agency found itself thwarted by the security features Apple had built into the phone – in particular, the requirement to enter a PIN to gain access. The FBI turned to Apple to request its help – and the tech firm refused. And so began a battle – in the courts and in the media.

Figure 1: Javvad Malik, AlienVault: "No-one in security or technology is actually saying they don't want to help law enforcement to go out and catch these criminals."

Black and white

"I think there are several angles to consider, when looking at the Apple/FBI debate," says Malik. "One of the challenges we have from a general perspective is, it's not really a black-and-white case. I think it's become quite emotional."

Unfortunately, this is often how the debate is framed, he says, with an appeal to emotion rather than reason, and with little room for nuance.

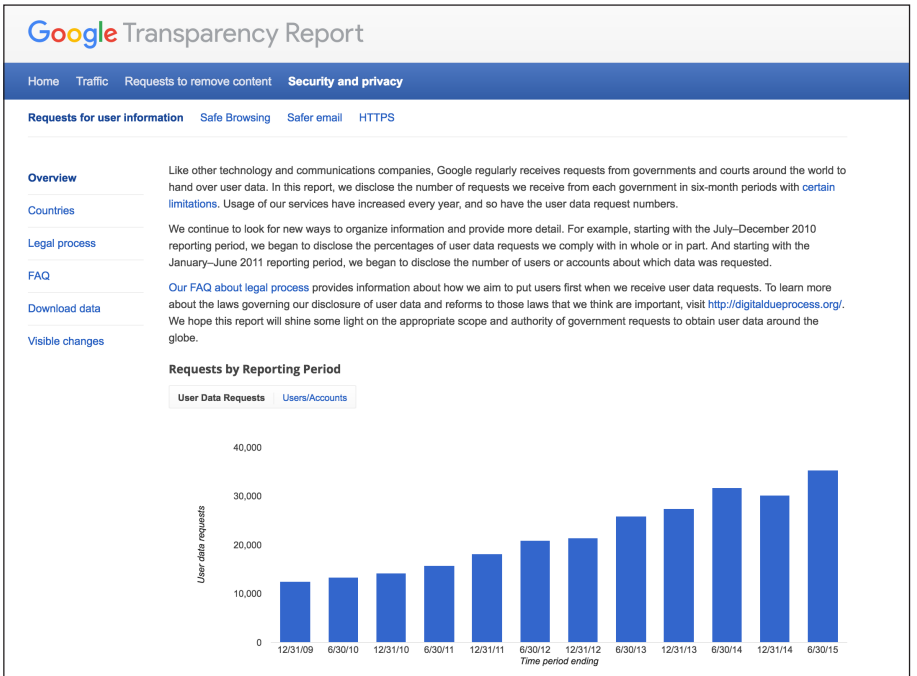


Figure 2: The tension between the authorities and tech companies has led many large firms to publish details about government requests for information in their transparency reports. This example is from Google. As laws in the US prevent the firms from disclosing details about certain types of request (because even the request itself is classified as secret), some companies include so-called 'canary' statements. These state that no requests were made under such laws. If the statement disappears from the transparency report, people can draw their own conclusions.

"The real discussion that needs to happen is, what's the best way that law enforcement can be helped by technology? Where is it appropriate, and where is it inappropriate?"

"If someone were to kill your family, or if someone was a threat to your loved ones, or if one of your children was kidnapped, would you not want law enforcement to have access to phones?" he says. "While that is a realistic scenario, I think it frames the discussion in a very black-and-white perspective. It forces the issue of either/or.

"I think no-one in security or technology is actually saying they don't want to help law enforcement to go out and catch these criminals," he adds. "The real discussion that needs to happen is, well, what's the best way that law enforcement can be helped by technology? Where is it appropriate, and where is it inappropriate?"

"It appears as if technology companies are just taking a stand, and saying, 'hey, we value our profits, or customer reputation, more highly than cooperating with law enforcement'"

Where to draw the line was the issue – and actually still is the issue, in some ways – in the dispute between Apple and the FBI over Farook's iPhone. The fact is, Apple co-operated with the agency to a considerable degree, including providing Farook's iCloud back-ups. This is something that wasn't always clear when the debate spilled out into the public arena.

"Sometimes you read coverage, or you hear opinions, and it appears as if technology companies are just taking a stand, and saying, 'hey, we value our profits, or customer reputation, more highly than co-operating with law enforcement'," says Malik. "I don't think that's the case at all. It's really about what they feel is the most appropriate way in which to co-operate."

Sticking point

So if Apple was co-operating, why did it stop? The sticking point came when the FBI wanted access not just to information that Apple held, but data that was on the phone and which would require changes – hacks, if you will – to the operating system to recover.

"Effectively the FBI were asking Apple to weaken – fundamentally weaken – the security of their operating system to allow the FBI access," explains Malik.

The FBI was unable to get past the iPhone's lock screen. The system used by Apple allows a small number of attempts at guessing the code before imposing a time delay between tries – a common security technique known as rate limiting. These delays can get quite large quite quickly – up to an hour – making a brute force attempt at unlocking the phone impractical. In addition, devices can be configured to wipe all data after 10 incorrect guesses.

It didn't help that the FBI made an error early on in the investigation. It suggested to San Bernardino County – the owner of the phone and Farook's employer – that it should request a reset of the iCloud password, in the hope of switching cloud back-ups on again. The data on the phone would then have been uploaded to Apple's servers. This didn't work and made data recovery far more difficult.

"I think anyone who's worked in technology knows that if you intentionally put in a back door into your software, it's guaranteed that sooner or later, [the secret] will escape"

Despite the popular image of US intelligence agencies as being all-powerful and equipped with technological capabilities beyond the dreams of mortals, it seems this was an insurmountable obstacle for the FBI. There are many rumours about whether the NSA has the ability to crack such security: as the US chief signals intelligence agency, this would be very much within its domain. Regardless – officially, at least – the FBI (strangely) did not ask for the NSA's assistance.

Baked-in security

As the passcode security is baked deep into the iOS operating system, Apple could not offer a simple work-around. After all, the whole point of having security like this is that it is not easily subverted. The FBI's solution was to ask Apple to create a special, one-off version of iOS with the rate limiting disabled. That's where Apple drew the line and said no.

In an open letter, Apple CEO Tim Cook wrote: "Up to this point, we have done everything that is both within our power and within the law to help them. But now the US Government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a back door to the iPhone."[3]

Malik agrees. "Some of us would say they were asking for a back door," he says. "I think anyone who's worked in technology – especially in the last decade, with everything connected and with all the vulnerabilities that exist, and with the advancements in analytics and those sorts of capabilities – knows that if you intentionally put in a back door into your software, it's guaranteed that sooner or later, [the secret] will escape. You can't put that genie back in the bottle. So it won't just be limited to law enforcement – the people who you don't want to have access

Figure 3: The iPhone lock screen that defeated the best efforts of the FBI – until the agency paid an estimated $1.2m for an exploit.

to it will eventually gain access to it, and then the things that they could do could be far more damaging to everybody."

It's not just cyber-criminals who might exploit that deliberate flaw. If Apple complied with the FBI's request, it's not far-fetched to predict that the law enforcement and intelligence agencies of other countries would be quick to follow. Apple, for example, has a significant presence in China.

"With a lot of analogue or traditional communications, there are geographical boundaries that wrap around it, so law enforcement operate within their own jurisdictions. With the digital age, the geographic boundaries, and hence the jurisdictions, become very, very convoluted"

"I think we need to step outside the black-and-white of asking do we want to stop criminals?" says Malik. "Well yes – but how we define criminals varies very differently around the world, and you put the technology companies in a very, very tough situation. We all have opinions of what are oppressive regimes, and some of them don't like any of their citizens to even blog anything detrimental about their leaders. Now, if technology companies were to starting handing over all of that information, then the consequences for people like that are far greater. You're effectively sentencing them to imprisonment or harsh treatment, or far worse. These are the global implications that need to be taken into consideration, because these are global companies, and the technology is used around the world."

Privileged information

There is, of course, another side to the story. After all, law enforcement organisations demanding access is nothing new. They have long had the ability to intercept telephone conversations or enter and search premises. So if they can leaf through our documents and tap our phone conversations, why should digital data be privileged?

"I think there's a couple of key differentiators," says Malik. "With a lot of analogue or traditional communications, there are some sort of geographical boundaries that wrap around it, to a degree, so law enforcement operate within their own jurisdictions. It was very easy to say, okay, this is a UK or a US issue, and we'll treat it as such. With the digital age, the geographic boundaries, and hence the jurisdictions, become very, very convoluted. So if an Iranian-based party is communicating with a Chinese-based party, but they're communicating through servers that are based in the US somewhere, and all of them are part of something nefarious, well, who actually has jurisdiction?"

He adds: "The second impact is that the advancements in big data, and the analytics behind it, have made it incredibly easy to conduct this surveillance in bulk, and indiscriminately."

The age-old argument that 'if you've nothing to hide, you've nothing to fear' rather breaks down in this technological new age, Malik believes. Because it's not just the data you knowingly store or share that you have to worry about. All of our technology-based activities are mapped and accompanied by metadata that we usually never see. But it's this metadata that is often of most interest to intelligence agencies, which use techniques such as traffic analysis and pattern recognition to identify data – and people – that may be of interest. With all of us subject to mass surveillance, we are all the prey of these algorithms.

In addition, Malik points out: "With people so dependent on technology to help them with absolutely everything, they divulge their most innermost, deepest, darkest desires. I'll type into Google major search terms that I might be too embarrassed to ask my doctor about. I've got a weird rash – well let me just ask Google first, because I feel that's more private, and that'll stay between us."

Subconsciously, he feels, people presume a level of privacy in digital communications.

"There is a kind of trust that they feel there, which is really evidenced by their behaviour and what they entrust to technology," he says. And partly this stems from a lack of awareness of how the technology operates and how much additional information it's collecting. He gives the example of geolocation. "You might use maps, but the average user isn't really consciously aware of all the places that are recording that data, and how a picture of your movements can be built up over time."

Not only do most people not realise that this metadata exists, and is being collected and stored, but they also have no control over it.

"At the moment there's a large amount of blind faith or trust put into the providers of the devices and the software, and the individual app manufacturers as well," he says. "It's a very thin membrane that actually protects that from going out into the wild wholesale, and this again, I think, is where this mass surveillance or implanting of back doors would have a really detrimental effect."

Trust in government

The Apple/FBI battle comes at a time when the tech industry and governments are drawing up battle lines over technologies such as end-to-end encryption in consumer products. The UK Government, in particular, has been vociferous in its demands that tech companies provide back doors for law enforcement. There have been other court cases, too.

"I think there's a certain degree of apathy as well – that I can protest to a degree, as long as I don't have to go out and stand in the cold and the rain"

Apple and the FBI faced each other in a case in New York where the law enforcement agency was, again, attempting to use the All Writs Act to compel Apple to unlock a phone by a self-confessed drug dealer. In that case, magistrate James Orenstein ruled that using the All Writs Act was inappropriate, and wrote: "The implications of the Government's position are so far-reaching – both in terms of what it would allow today and what it implies about Congressional intent in 1789 – as to produce impermissibly absurd results." As Apple had no part in

the drug dealer's wrongdoing, Orenstein ruled, it was impossible to justify "imposing on Apple the obligation to assist the Government's investigation against its will".

Coming on top of the Snowden revelations, how is all this affecting the trust relationship between citizens and governments? Malik doesn't think there's a clear-cut answer to that.

"The Snowden revelations came as somewhat of a surprise for some," he says. "Other people were not surprised. Then there's a whole bunch of people that were surprised, but acted as if they weren't. I think these sort of things happen quite frequently. Over time, when you see documents, as they become declassified, people are like, 'Oh shock! – the Government's done this'. So there's always been this element of mistrust. But I also think, speaking as a Brit, I think there's a certain degree of apathy as well – that I can protest to a degree, as long as I don't have to go out and stand in the cold and the rain."

However, there are consequences that can be detected. Malik points to reports that, since the Snowden revelations, the number of searches people make online relating to terrorism and other sensitive subjects have decreased considerably. It seems that people are concerned that the searches will be spotted and mark them as 'persons of interest'. It has become a form of self-censorship.

Drawing a line

As for the tech companies, the question of what information they will and won't supply to the authorities is not going to go away. As we know from their own transparency reports, large companies such as Google, Facebook, Microsoft and, yes, even Apple, regularly provide law enforcement with user data, as they are obliged to by the laws of the countries in which they operate.

"If a tech company is holding a bunch of customer data, and law enforcement approaches it, the first step should be to ask if it is a valid request"

We'll never know how much data they surrender under rules that come complete with gagging orders. The difficult issues arise when the laws are less clear – as in the FBI's attempt to exploit the 1789 All Writs Act – and where they are absent. How do tech firms decide where the line should be drawn in terms of handing over data? And is that really an issue for them to decide?

"The lines keep on evolving to a degree," says Malik. "If a tech company is holding a bunch of customer data, and law enforcement approaches them, I think the first step should be to ask if it is a valid request. And they should have a published method by which, if you're law enforcement in any country, then these are the requirements that are needed. It may be a court order or something of that sort."

There should also be a process around disclosure, he adds, dealing with issues such as whether the customer is notified, whether customers themselves should be the ones to surrender the data, making the tech company simply an intermediary, and so on. In effect, much of this would be on a case-by-case basis, says Malik, "rather than saying, well okay, just bring us one court order that gives you carte blanche access to every single one of our hundreds or thousands of customers, and you can come in and out and check the data at will. I think that's really where the line is drawn, and that's where Apple has drawn the line."

A matter for the courts

Ultimately, much of this will be decided in court. The FBI attempted to force Apple to co-operate by invoking the All Writs Act, which compels people and organisations to assist law enforcement investigations. Unusually, in such matters, the FBI's case against Apple was a civil one. The FBI won its suit. Apple then appealed, but before a judgment could be reached, the FBI dropped the case.

Superficially, the reason appeared simple – the FBI had finally gained access to the data on the iPhone. It had bought – for a rumoured $1.2m – an exploit from an unnamed company that somehow bypassed the passcode security. Not only has the FBI refused to name who supplied the technique, it has refused to give details of the vulnerability it exploited, potentially leaving other iPhone 5C users at risk. The agency claims that the exploit runs only on the 5C model and only on the specific version of iOS that Farook was using.

There are other interpretations of what happened – especially in the light of the FBI's later admission that it had found no useful information on the phone. This, in itself, was not surprising. While Farook had stopped making iCloud back-ups a few weeks before the shooting incident – which is why the FBI needed access to the phone itself – this may have been a coincidence. Farook personally owned two other phones, both of which he was careful to destroy before the incident. It always seemed unlikely that any incriminating evidence was going to be found on the iPhone, rather than the destroyed devices.

"The optimist in me believes that Apple would have won the case, and set a precedent against law enforcement. But then part of me is also equally terrified that maybe they could have lost"

So why the court battle? This is where the story tends to descend into opinion and punditry. Nonetheless, there is a popular train of thought that suggests the FBI wanted to leverage a high-profile incident in order to set a precedent. A true cynic would suggest that, given the level of anti-Muslim feeling in the US and the emotions inevitably raised by anything connected with terrorism, the FBI may have believed it would face little opposition in making its demands. Any tech company that stood in its way would run the risk of seeming to be on the side of terrorists – which makes Apple's stand all the more remarkable.

Many people were disappointed that the case didn't run its full course, with all possible appeals being exhausted. That would have helped to provide some clarity.

"I think it is a shame," says Malik, "because the optimist in me believes that Apple would have won the case and set a precedent against law enforcement. But then part of me is also equally terrified that maybe they could have lost, because once you go to court, you're never really sure how things will pan out."

Oversharing

The information that intelligence and law enforcement agencies desire doesn't get onto mobile devices and social networks by accident. We put it there. So while some people might harbour an expectation of privacy, at the same time many of them are busily oversharing – in other words, maybe they're not as bothered about privacy as previous generations (or those working in the information security business). Certainly, there seems to be little thought given as to what information they're giving away.

"We were the first generation to be exposed to this type of technology, and we're the generation that made all the mistakes," says Malik. Oversharing and injudicious use of social networks are typical of those mistakes. But now, he says, there's a second generation where the sharing is often about monetisation and marketing. "A lot of people are in it for the fame, or trying to use it to build a career. We're at this critical turning point where it's vital that people that have gone through and made those mistakes, and those who are aware of the tech side, to really educate and inform users of the perils and the dangers. We've already seen things like cyber-bullying, for example, as one of the uglier trends that have emerged as a result of this technology."

The general public's desire for privacy-enhancing technologies is notable by its absence. And the technologies are available. Silent Circle, for example, has launched encrypted messaging services and the Black Phone encrypted smartphone, which have been promoted heavily since the Snowden leaks. But there hasn't been widespread adoption – these are still very niche products. And mainstream tech companies rarely market themselves on the basis of how secure their products are. So is this an untapped market opportunity, or something that just doesn't have traction with the public?

"I think it's definitely an opportunity," says Malik. "I think the overall positioning in the market is very immature. So there isn't a big rush to go out and buy things like the Black Phone. And I think there's this narrative around that anyone using something like a Black Phone or encryption is inherently up to no good. And that's the narrative that I think needs to change."

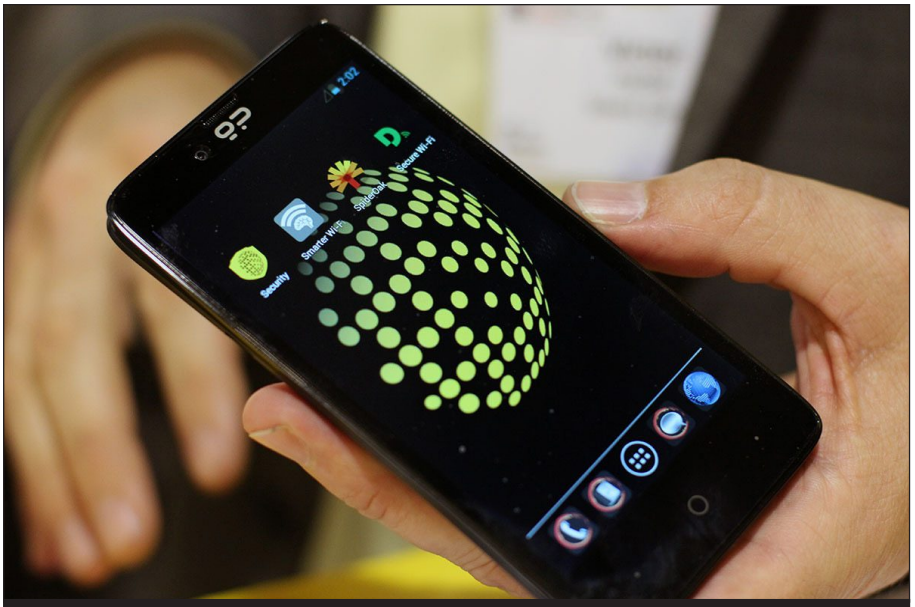


Figure 4: The Black Phone provides built-in encryption but has found only a niche market.

"It's really a user issue – letting users make informed decisions, whether they actually even want to use those platforms or not, and if they do, what's the best way"

He points out that there was a time when cars were sold on the basis of their performance or speed, but now you'll more often see manufacturers boasting of their safety or economy. Technology needs to go through a similar shift. And tech firms could play a major role by building in end-to-end encryption capabilities for communications and strong on-device encryption for storage. And then they need to make it a selling point.

During the Apple/FBI spat, the law enforcement agency accused Apple of exploiting a terrorist attack for publicity. It was a cheap shot, but the fact is that no-one was left unaware that Apple provides strong security on its products. Whether tech companies have a will to provide these kind of capabilities is another matter.

"The challenge, really, is for the middle to smaller client technology companies," says Malik. "Building in all this security takes time and resources and costs. So they're effectively trying to balance out how much they actually put into security versus how much profit they're making, and I think that's one of the big challenges that needs to be overcome, from our overall technology perspective."

Ultimately, however secure tech companies make their products, our privacy depends on how we use them. And many of the services we use, such as Facebook, are built on the concept of oversharing.

"It's really a user issue," says Malik, "and awareness and education – and letting users make informed decisions, whether they actually even want to use those platforms or not, and if they do, what's the best way."

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Network Security and its sister publication Computer Fraud & Security. He also blogs and podcasts about security at Contrarisk.com.

References

1. 'Clipper chip'. Wikipedia. Accessed May 2016. https://en.wikipedia.org/wiki/Clipper_chip.
2. '2015 San Bernardino attack'. Wikipedia. May 2016. https://en.wikipedia.org/wiki/2015_San_Bernardino_attack.
3. Cook, Tim. 'A message to our customers'. Apple, 16 Jan 2016. Accessed May 2016. www.apple.com/customer-letter/.

Holding the fort: a business case for testing security


Sameer Dixit

Sameer Dixit, Spirent

With the cost of breaches sky-rocketing year on year, many of the perimeter security vendors – or firewall companies – that are your organisation's first line of defence are failing and being breached themselves. It's now more important than ever to subject your critical infrastructure to real world threat modelling and penetration testing. This helps identify the security gaps in your network, wireless, mobile and web applications as 80-85% of these tests reveals critical security flaws.

What is the true cost of security? A typical ROI calculation compares the pounds spent with the pounds gained in return: but when it comes to security, you can only compare spend with a hypothetical figure of what might have been lost. In essence, you are investing to lower risk, much like paying the legal department to reduce liability.

Installing security solutions is no guarantee of protection and the more that is installed, the more complex the situation and the harder it becomes to predict outcomes. Instead we must resort to testing: but inadequate testing can build a false sense of security and cause more problems than not testing at all. What is needed is a test platform designed to create truly realistic conditions, coupled with industry best practices developed through experience and training.

Inadequate protection

Gartner recently estimated that the cost of downtime for computer networks ranges from around $42,000 per hour to 10 times that or more for a financial services company trading on Wall Street.[1] The loss of HIPAA data (Health Insurance Portability and Accountability Act of 1996) has cost some companies as much as $1,000 per record in the resulting lawsuits.

The cost to businesses of exposing data such as social security and payment card numbers rose to an average of $7.2m per incident, according to a 2013 study. The most expensive incident cost an unidentified company $35.3m, an increase of 15% from the costliest breach a year earlier, according to a report from the Ponemon Institute.[2] Malicious attacks increased 7% from the previous year, with the costs of such attacks jumping 48% to an average of $318 per compromised record.

The true return on investment in security has to be calculated in terms of an estimate of potential losses and the probabilities of suffering those losses. This is a complex calculation because there are so many distinct yet interlinked types of loss in a typical operation. These losses include:

- **Revenue.** For revenue-generating systems, such as e-commerce websites, revenue per hour can be estimated from historical data. Less downtime means less cost.
- **Productivity.** Crippled IT systems amount to lost hours of work.
- **Data loss.** If data is wiped, work is lost for the duration of the restore process. If the back-ups too are destroyed, this could be a lengthy process.
- **Data compromise.** The exposure of sensitive user information invokes costly lawsuits. Compromised personal data – such as health data, National Insurance numbers, SSN, credit card information – will drive customers away.
- **Goodwill.** This includes a company's reputation with existing and potential customers and with partners, vendors and investors.

Once these potential losses have been estimated – usually in terms of a realistic minimum to maximum scale – the cost of protection can be compared to the likely cost of loss. Experience suggests a figure around 30-40% of the anticipated cost of the loss is the maximum that need be assigned for protection, but the actual cost of a security solution typically falls well below that maximum.

Trust but verify

Every organisation already has some measure of security in place, but the number of costly breaches being reported suggests that the security is often not enough. What needs to be done to assure yourself and your stakeholders that you are adequately protected? The answer is: trust but verify.

There is an old saying from the Middle East: "Trust in God, but tether your camel". You can be sure that any security vendor will present its products in the best possible light, so it is ultimately up to customers to decide whether the solution really meets their needs. Even if the vendor's claims are completely accurate, its QA department cannot possibly test every combination of features under all possible scenarios that a customer might need. You have to know what testing was actually performed to justify the numbers in the brochure. Did the company test against all of the thousands of known attacks and vulnerabilities? Did it use 'negative testing' to recreate unpredict-

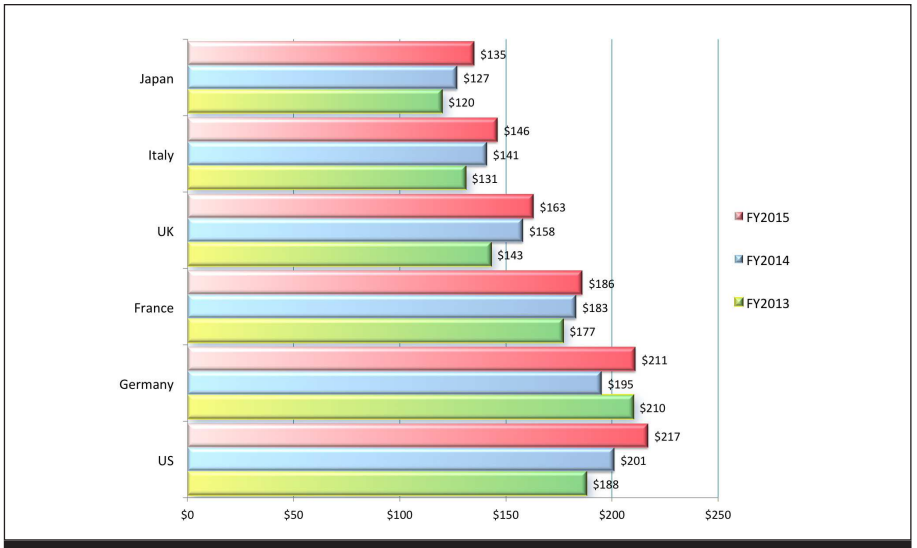


Figure 1: The average per capita cost of data breach over three years. Source: Ponemon Institute/IBM.

able scenarios that are frequently the cause of catastrophic and costly breaches and failures? (Negative testing includes testing against programmed logic, phishing defences, input validation controls, human error inputs, such as mis-keying or inserting a zero instead of a capital O, to see if these cause a system crash.)

Do not forget that a security solution not only has to protect your organisation, it must also remain transparent to the workforce. A rock-solid security process that demands tiresome and time-consuming effort will reduce productivity and be bypassed by busy staff. Next-generation firewalls provide many new capabilities, but they may come at the cost of performance. Only testing will tell the true story. A suitable test platform and threat modelling exercise will subject your network and web properties to be modelled in the test lab with real world threats and identify the potential gaps in security. Deploying a new device in the network could expose limits in the device, or potential security risks in your network. That is critical information that should ideally be discovered by testing before purchase – certainly before deployment in a production environment.

Inadequate testing

Inadequate testing can be worse than no testing at all since it encourages a false sense of security. If you head off into the wilderness in a 4x4 you want to be sure that it has been tested under off-road conditions, not just on a highway test track.

In the so-called 'Age of the Customer', greater attention is being paid to exhaustive pre-testing of products and services before they face the ultimate test in consumers' hands. But nevertheless, some people still see testing as an afterthought, just a way of confirming good design. If your test tools are unable to recreate a realistic model of the target environment, you risk making negative headlines. Obvious short cuts to avoid include:

- Using a production network out of hours is nothing like its operating environment.
- Home-grown scripts running on a CPU don't have the power or sophistication to recreate the full diversity and complexity of a typical production network.
- Open-source freeware can be useful for troubleshooting problems, fine-tuning protocol settings, and conducting basic functional and throughput tests, but it will not be capable of testing the latest security devices' deep packet inspection (DPI) and app-aware features.
- Using a packet blaster. This is for testing line-rate device performance and basic functionality. It is not designed or intended to test performance, availability, security and scalability.

True testing

Realistic testing means recreating the solution's working environment end-to-end from provider to end user. This not only means using the right test tools, it also requires experience or training for accurate evaluation of performance, availability, security, and scalability. Having modelled the working environment correctly, you must also recreate both normal and possible extreme operating conditions.

This means taking into consideration three further elements:

- **User behaviour.** Realistic testing requires the flexibility and sophistication to emulate a wide range of user behaviours, both normal and malicious. For security testing, this includes emulating the thousands of known attacks using real application traffic with the full range of versions and possible endpoints.
- **Converged traffic.** Realistic testing requires emulating stateful traffic across hundreds of ports. For security testing, this includes the ability to use 'fuzzing tests' and custom tests for proprietary protocols to stress DPI, application awareness and other processor-intensive capabilities.
- **Network operating conditions.** Realistic testing requires the power and complexity to emulate the dynamic, time-varying conditions found on deployed, production networks. For security testing, this includes the extreme congestion typical of DDoS attacks.

Choosing a partner

Putting all these requirements together, and understanding which are most critical for your own operation, allows me to suggest some key points to consider when choosing a testing partner.

One: testing should be built on experience, so choose a vendor with testing as a core competence rather than relying on open-source freeware or an ad hoc solution. Choose a partner that has a globally established name in the security, testing and measurement industry with verifiable experience and expertise.

Two: the test platform must have the power and sophistication to support all the suggested elements of test realism – real user behaviour, real converged traffic, and real network conditions – to be able

to test the performance, availability, security and scalability of the device or system under stress.

Three: verify that the test platform specifically stresses known software vulnerability triggers. It should access a constantly updated library of the thousands of known attacks. The platform must have the power to replicate known and potential DDoS attacks at Internet scale, together with the flexibility to test DPI even on proprietary protocols and support for negative testing through fuzzing.

Four: the system should support the latest automation and built-in GUI-based tools for simplifying and automating standards-based and customisable test cases. Reducing repetitive manual work will reduce human error as well as allowing more time for assiduous test development.

Five: verify that the testing solution is backed by a team of experienced pen-testers and security researchers that are actively researching new emerging threats and enhancing the test solutions' capabilities to test against newer vulnerabilities.

Conclusion

If you want to know what real security feels like, do not skimp on testing. Due diligence means more than simply choosing a solution on the basis of a list of data sheet specifications.

If you wish to validate security vendor claims, first you need to verify the suitability of the solution and services for your unique organisation, apps, network and operation, then quantify the level of protection you will need when you go live, then test the solution under real world conditions.

This type of testing is key to knowing how much you can trust your security solution – so the choice of testing partner is every bit as important as your choice of security vendor.

About the author

Sameer Dixit is senior director for security consulting at Spirent Communications and has more than 15 years experience in penetration testing and security research. Dixit leads Spirent's ethical hacking and security research team – Spirent Security Labs. Prior to Spirent, he worked for leading security companies such as Trustwave-SpiderLabs and Cenzic, where he led the penetration testing, vulnerability scanning and managed security testing services team. Dixit has contributed research for OWASP, been quoted in various industry-leading security and business publications, and regularly speaks at cyber-security events. He blogs on emerging web and mobile security trends.

References

1. Pisello, T; Quirk, B. 'How to quantify downtime'. Network World, 5 Jan 2004. Accessed May 2016. www.networkworld.com/article/2329877/infrastructure-management/how-to-quantify-downtime.html.
2. 'Ponemon Institute's 2015 Global Cost of Data Breach study reveals average cost of data breach reaches record levels'. IBM, 27 May 2015. Accessed May 2016. www-03.ibm.com/press/us/en/pressrelease/47022.wss.

The SIP security fallacy


Paul German

Paul German, VoipSec

There is no such thing as static security – all security products become vulnerable over time as the threat landscape evolves. Any 'deploy once, update infrequently or never' security solution is inherently flawed. Which is why every switched-on organisation routinely updates its anti-virus and anti-malware solutions, hardens its infrastructure and updates its policies. So why is SIP security still based upon a one-off implementation of a Session Border Controller (SBC)?

From denial of service attacks to toll fraud, SIP trunking is inherently vulnerable. And in an era of near-continuous security breaches, that vulnerability continues to change and escalate. No technology or communications environment is static and SIP security should be treated with the same urgency as anti-virus and infrastructure hardening.

The breaches go on

Another day, another security breach. The theft of 15 million T-Mobile customers' data from credit-checking firm Experian, the exposure of the personal data of US-based Uber drivers, the hack of Samsung Pay, the denial of service (DoS) attack on HSBC – all of these events have occurred within very recent history. The scale of hacking and data theft is unprecedented and new attack vectors are continually being found and compromised.

Today's threat levels are high and – given the constant publicity and public scrutiny – only the most foolhardy organisation would ignore the need to safeguard infrastructure. Yet in what is a continually changing and evolving threat landscape, inconsistencies in security policies and practices are creating new vulnerabilities.

"Why are organisations totally committed to continuously updating anti-virus (AV) and anti-malware solutions yet will happily install a Session Border Controller (SBC) to protect VoIP calls and never consider it again?"

Why, for example, are organisations totally committed to continuously updat-

ing anti-virus (AV) and anti-malware solutions yet will happily install a Session Border Controller (SBC) to protect VoIP calls and never consider it again?

If there is one thing that every security expert will confirm, it is the continuously changing nature of the threat landscape – and a security product's ability to safeguard a company declines from day one. In an era of near-ubiquitous VoIP calls, when companies are routinely falling prey to toll fraud and denial of service attacks, it is time to ask why network providers and security vendors continue to downplay the vulnerability of SIP.

Static fallacy

The deploy once, update many times model adopted by AV, web security and email security over the past two decades is well established and organisations recognise the clear vulnerabilities associated with failing to update routinely. Companies understand the importance of buying not just a security product but a vendor's continuous research into emerging threats and a commitment not only to routine updates but also emergency patches in response to new hacking vulnerabilities. In effect, when it comes to a continuously changing security situation, organisations recognise the need to buy products and solutions that utilise research, existing users and community to stay ahead of the hacker.

"Why are other aspects of the communications network and infrastructure, including routers and switches, still subject to the static – implement once, update never – approach?"

So why are other aspects of the communications network and infrastructure, including routers and switches, still subject to the static – implement once, update never – approach? Does this mean these areas are impregnable once protected? While some vendors may like to imply this is the case – it is not. Toll fraud and denial of service cost businesses £25.5bn every year globally – £1.2bn in the UK alone, and, again, the threats continually evolve. For example, hackers are routinely undertaking port scanning in the hope of finding a way in – any organisation that has left SIP ports open is likely to be found out, and compromised, very quickly.

Complex sell

The challenge is that, for any solution provider – whether vendor or reseller – the objective is to minimise any sales inhibitors. And in the SIP trunking market that inhibitor to date has been security and its associated costs. In a market where the move from ISDN to SIP and Unified Communications (UC) is compelling on the basis of both cost reduction and improved features and control, why would anyone want to rock the boat by mentioning the inherent security risks?

"With 84% of UK businesses considered to be unsafe from hacking, according to NEC, the implications are significant and extend far beyond the obvious financial costs of huge phone bills"

SIP trunking vendors often fudge concerns by citing their own SBC investment: if they are secure, their customers are secure. But take a closer look at the contract and it becomes very clear that in the event of a breach that results in toll fraud, denial of service or data loss, the provider is not liable for the associated cost.

VARs, meanwhile, when faced with a switched-on customer raising the thorny security issue have had no option but to recommend a customer source its own security – at a significant cost – and stuff the proposal full of security caveats. In the vast majority of SIP deployments the onus is still on the customer to ensure the SIP trunk is secure – whether they know it or not. Clearly, the entire process is unsatisfactory for all involved.

Scale of attack

The fact is that in a constantly evolving threat landscape, security has to be considered – this head in the sand approach adopted by many SIP trunk providers and resellers is simply not good enough given the scale of attack being experienced by UK businesses.

"From eavesdropping sensitive communications with malicious intent to misrepresenting identity, authority, rights and content or gaining access to private company and customer contacts, hackers are increasingly looking for more than basic call jacking"

Security consultancy Nettitude's recent report revealed that attacks on VoIP servers represented 67% of all attacks it recorded against UK-based services – in contrast, SQL was the second most attacked service, accounting for just 4% of the overall traffic. With 84% of UK businesses considered to be unsafe from hacking according to NEC, the implications are significant and extend far beyond the obvious financial costs of huge phone bills or the increasingly common Telephone Denial of Service threats, also known as ransom events used to extort money.

From eavesdropping sensitive communications with malicious intent such as harassment or extortion to misrepresent-

ing identity, authority, rights and content – such as modifying billing records – or gaining access to private company and customer contacts, hackers are increasingly looking for more than basic call jacking.

Cloud-based intelligence

The good news is that the days of expensive, hardware SBCs are over. The latest generation of cloud-based, 'freemium' voice firewall security products can be downloaded and deployed within minutes, securing the voice network without impacting the compelling SIP trunking cost benefits. Essentially these virtual SBCs provide customers with the first tier in voice security, providing the foundation for the defence-in-depth model that has been applied to secure data networks over the last decade.

"In a constantly evolving threat landscape, security has to be considered – this head in the sand approach adopted by many SIP trunk providers and resellers is simply not good enough given the scale of attack"

Indeed, in all forms security has had to keep ahead of the hacker and VoIP is no different. As with anti-virus, intrusion protection/detection, web and email security this threat landscape has to be monitored and understood and any newly identified risks mitigated.

There are proven ways to stay ahead of the hacker; cloud-based VoIP security allows organisations – and providers – to apply the approach being taken by AV, email and web security vendors to:

- **Identify common threats** and provide solutions to mitigate the risks associated with those threats.
- **Build teams to understand where new threats are going to come from** and develop solutions to address those.
- **Grow communities** whose shared learning and insight will provide greater visibility into the wider threat landscape.

Moreover, this approach heralds a commercial game changer for the SIP trunk market: a move from Capex-based solutions to Opex, with virtualised versions of a voice security infrastructure that are updated in real-time on subscription.

Ahead of the game

The cyber-security market is set to be worth $170.21bn by 2020 – with a strong bias towards securing email, desktops and web services. Yet while the adoption of VoIP is now at record levels, SIP security investment remains low. When hackers are looking for the easiest way in, this lack of protection is an open invitation.

"Static security does not work; it is time for the SIP security industry to face up to its responsibilities and embrace a process of continual update"

The reality is that SBCs provide an entry level of security – but, like any other security product, they need to evolve. And that means SBC providers need to be making a continuous investment in security research and providing routine updates in order to deliver a reactive, real time and intelligent level of security to protect against these new world threats.

Organisations – and providers – need a change of attitude to SIP security. In a constantly evolving threat landscape no one knows what is coming and the onus is on both vendors and businesses to ensure they are in the best possible position to both safeguard data and protect against expensive toll fraud attacks. The constant change process has become a fundamental aspect of successful security – and that needs to be applied across the board, not just to AV. Static security does not work; it is time for the SIP security industry to face up to its responsibilities and embrace a process of continual update that will truly safeguard organisations tomorrow – not just today.

About the author

Paul German is founder & CEO of VoipSec, which specialises in VoIP security. He has over 18 years' experience in the areas of unified communications, voice and network security, having worked with a broad range of organisations including Cisco and most recently leading the EMEA business for Sipera Systems.

EVENTS CALENDAR

19-22 July 2016
Privacy Enhancing Technology Symposium
Darmstadt, Germany
www.petsymposium.org

20–22 July 2016
RSA Asia Pacific & Japan
Marina Bay Sands, Singapore
www.rsaconference.com/events/ap16

26–28 July 2016
Secrypt – International Conference on Security and Cryptography
Lisbon, Portugal
www.secrypt.icete.org

30 July–4 August 2016
Black Hat USA
Las Vegas, US
www.blackhat.com

4–7 August 2016
DefCon
Las Vegas, US
www.defcon.org

10–12 August 2016
25th USENIX Security Symposium
Austin, TX, US
www.usenix.org/conference/usenixsecurity16

31 August–2 September 2016
ARES – International Conference on Availability, Reliability and Security
Salzburg, Austria
www.ares-conference.eu/conference/

19–20 September 2016
Information Security Network
Reading, UK
https://thenetwork-group.com/information-security-network/