ELSEVIER

computer FRAUD & SECURITY

ISSN 1361-3723 May 2019

www.computerfraudandsecurity.com

Featured in this issue:

How readable are data breach notifications?

Data breaches – where protected data that is considered sensitive and confidential has been accessed in an unauthorised manner – present a growing threat to society and organisations.

While much of the focus to date has been on technical countermeasures, we also need greater insights into the readability of the notification response used by firms to alert affected consumers after a suspected incident has taken place. Stephen Jackson of the University of London examines ways in which we can judge how comprehensible breach notifications are and how we can go about improving them.

Full story on page 6…

Gamification as a winning cyber security strategy

Just like in some video games, consumers and business leaders find themselves battling the consequences of interconnectivity and are trying to keep opponents from exploiting their information and damaging their reputation.

In this 'game of protection' to balance defensive and offensive security techniques, now is the time for CISOs and business leaders to reach for a new cyber security manual – one that leverages gamification. This is the process of exploiting game-like elements to improve information retention and the application of skills, explains Brad Wolfenden of Circadence.

Full story on page 9…

IoT security: could careless talk cost livelihoods?

The rise of the Internet of Things (IoT) promises exciting capabilities for business but could it usher in risks that are difficult to assess, let alone deal with?

Unsecured IoT systems could be the equivalent of careless talk giving away company secrets and endangering livelihoods. IoT-enabled devices behind cutting-edge consumer and business products must talk securely to the company's core IT and business systems. Without this secure conversation, IoT's learning capabilities could simply enable hackers to carry out wider-scale attacks, explains Marc Sollars of Teneo.

Full story on page 12…

Church scammed as FBI warns of major rise in BEC fraud

A US church has lost $1.75m after being targeted in a business email compromise (BEC) scam. Meanwhile, the FBI has warned we can expect more of the same, with BEC losses having surged to $1.2bn last year.

The Saint Ambrose Catholic Parish in Brunswick, Ohio was defrauded by scammers who were apparently aware the church was making regular payments to a local construction business for renovation work. The first the church knew of a problem was when the construction firm, Marous Brothers, called to ask why the previous two months' payments,

Continued on page 3...

Contents

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

Publishing Director: Sarah Jenkins
Editor: Steve Mansfield-Devine
E-mail: infosec@webvivant.com

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

Subscription Information
An annual subscription to Computer Fraud & Security includes 12 issues and online access for up to 5 users. Subscriptions run for 12 months, from the date payment is received.

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

12986
Digitally Produced by
Mayfield Press (Oxford) Limited

Editorial

Rape victims in the UK are being told that they must surrender access to their phones and social media accounts or risk having their cases withdrawn.

According to the Crown Prosecution Service (CPS), new consent forms that have been introduced do not represent a new policy but an attempt to standardise an approach across all police forces. But they have drawn widespread criticism – not least because there is little information on how personal, and sometimes very intimate, information will be treated, other than bland assurances that the data will only be used as part of "reasonable lines of enquiry". Unfortunately, 'reasonable' is a dangerously vague term.

On the one hand, the arguments for the 'national disclosure improvement plan' might seem logical. The move was prompted by the collapse of a number of high-profile rape cases in 2017 when evidence, based on the victims' communications via text, email and social media, cast doubt on their allegations. One can understand that prosecutors don't want to waste time and public money on cases where the alleged victim is being less than completely open.

The CPS has emphasised that providing access to accounts is at the discretion of the complainant, who can not only refuse but also submit reasons for doing so. Or the complainant can specify what data or time periods she believes to be relevant and limit the search to those. The CPS has said: "We recognise that only the reasonable lines of enquiry should be pursued to avoid unnecessary intrusion into the personal lives of individuals. Police officers fill in what information they will look for before obtaining a signature."

The problem is that this is all one-sided and there is still much that is vague. Worse, this process carries an implicit assumption that the accuser may be lying.

One would hope that searches of social media and communications would be limited to concrete facts pertinent to the case – for example, friendly exchanges between accuser and accused after the assault is said to have taken place, or evidence that the two people could not have been in the same place at the same time.

But who's to say that prosecutors won't amass 'evidence' of the complainant's character, attitudes and behaviour to provide an excuse not to proceed with a prosecution? Because the sad fact is that only 1.7% of reported rapes were prosecuted in 2018 and 40% of cases were abandoned with the comment "evidential difficulties". There is no epidemic of false rape claims. Victims must already fight hard to get their cases taken seriously and now a handful of failed cases make prosecution even more difficult.

The phrase 'you have nothing to fear if you have nothing to hide' has never been true. The problem with private data is that it's slippery stuff, open to interpretation. Victims will be disinclined to report attacks if they think their private lives are going to be trawled for evidence against them.

There are also questions about how this data will be stored and used. How long will it be retained? Will complainants be told what personal data has been retrieved and how it has been interpreted? Will decisions based on this private data be fully transparent? And will the accused face similar treatment – not just having to provide access to private communications but face consequences if this is denied?

Women claiming to have been victims of rape are being made to feel that they are acting in an unreasonable and suspicious manner – one that could undermine their entire case – if they don't allow access by the authorities to communications they might rightly regard as intimate and private. That is a dangerous precedent.

– Steve Mansfield-Devine

...Continued from front page
totalling $1.75m, had not been paid. The surprise was all the greater because the church had been receiving its regular, standard notifications from its bank that payments were going out as normal.

An investigation by the FBI found that someone at the church had been duped into believing that Marous Brothers had changed its banking details and wiring instructions – a classic BEC tactic. It's unclear how this was done, but it seems that two email accounts were compromised, possibly via phishing or keylogging malware. The church has submitted an insurance claim, but at the time of writing there was no confirmation that it would be reimbursed.

The recent '2018 Internet Crime Report' from the FBI's Internet Crime Complaint Centre (IC3) says that the agency dealt with more than 350,000 fraud and cybercrime incidents that resulted in losses of over $2.7bn, around half of which were BEC scams. Just over 20,000 people made complaints to IC3 about BEC or email account compromise (EAC) scams that totalled $1.2bn – well ahead of the next-biggest categories, confidence fraud and romance scams ($362m) and investment fraud ($253m). Tech support scams, extortion (including ransomware) and payroll diversion also featured significantly in the centre's figures.

The IC3 report is based on data from complaints made by the general public, mostly via the centre's website. Given that many people are too embarrassed to report being the victim of fraud, or feel that there is little point, the real scale of the problem is certain to be much larger.

According to the report: "BEC and EAC are constantly evolving as scammers become more sophisticated. In 2013, BEC/EAC scams routinely began with the hacking or spoofing of the email accounts of chief executive officers or chief financial officers and fraudulent emails were sent requesting wire payments be sent to fraudulent locations. Through the years, the scam has seen personal emails compromised, vendor emails compromised, spoofed lawyer email accounts, requests for W-2 [tax] information, and the targeting of the real estate sector."

The FBI report is here: http://bit.ly/2H5Yt8f.

Meanwhile, Proofpoint has published a study looking at BEC in the financial services sector – an increasingly popular target for scammers. Its '2019 Email Fraud in Financial Services' report analysed more than 160 billion emails sent in the two years 2017-2018 and reveals a relatively high level of sophistication among the attackers in terms of tailoring their emails for this sector.

"Wire-transfer scams are a large component of email fraud in the financial services industry," the report says. "Over the past two years, the top subject categories used to target financial services firms have included 'payment', 'request' and 'urgent'. Payment-related subject lines such as 'payment status', 'payment request' and 'swift transfer' were twice as common among financial services firms. They accounted for 10% of total messages vs just 5% across all industries."

Domain spoofing, in which the scammers' emails are made to look as though they are coming from legitimate sources – often from within the target organisation itself – was also very common. Nearly two-fifths (39%) of emails sent from financial services domains in Q4 2018 were categorised by Proofpoint as suspicious or unverified. A significant proportion of BEC emails are sent on Monday mornings – partly to avoid the suspicion that might attach to messages sent outside office hours but also, perhaps, to take advantage of people's more relaxed attitudes immediately following the weekend.

The report is here: http://bit.ly/2vKFucW.

Finally, nine men were arrested in the US on charges related to BEC and romance scams plus fraud involving a Russian oil deal, all of which are said to have netted them $3.5m.

"The common denominator in all three schemes was the defendants' alleged fleecing of their victims through fictitious online identities," said US Attorney Geoffrey Berman in a statement.

Dark markets busted

Two more dark markets – underground marketplaces operating via the dark web – have been taken down by law enforcement agencies.

Investigators in Germany, the Netherlands and the US collaborated to take down the Wall Street Market (WSM), with arrests of three German nationals and a Brazilian man, all of whom are in custody in Germany. The WSM was one of the world's largest dark markets, trading in illegal drugs, counterfeit goods and malware. The market, which operated in six languages, had an estimated 5,400 vendors selling to 1.15 million customers worldwide.

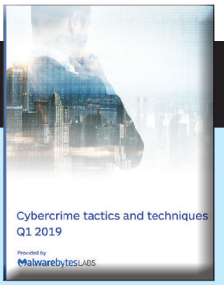
The WSM was run for three years, but it's alleged that the three German operators were in the throes of executing an 'exit scam'. This is where they abandon the site while stealing all crypto-currency funds held in escrow and user accounts. According to prosecutors, these three men diverted $11m worth of virtual currency into their own accounts. The defendants are facing charges in both Germany and the US. A further two people, accused of selling narcotics via WSM, have been arrested in Los Angeles.

As the takedown operation was in progress, one of the site's moderators, going by the handle Med3l1n, began contacting vendors and customers, threatening to reveal details of their illicit activities unless they paid a ransom – typically 0.05 bitcoins (around $280). The US Justice Department alleges that Med3l1n is Marcos Paulo De Oliveira-Annibale of Sao Paulo, Brazil, who has been indicted in the US District Court in Sacramento, California. He's also facing federal drug distribution and money laundering charges.

Meanwhile, in Finland, the country's Customs authority said it had shutdown the servers of Silkkitie, also known as the Valhalla Marketplace, which had been operating since 2013. There are no reports of arrests although the Finnish authorities said that the takeover of the servers had resulted in the seizure of a significant amount of Bitcoin crypto-currency. They also commented that the operators of the site had been seen moving to other dark websites, including WSM.

"These two investigations show the importance of law enforcement co-operation at an international level and demonstrate that illegal activity on the dark web is not as anonymous as criminals may think," said Europol executive director, Catherine De Bolle.

Report Analysis



Malwarebytes Labs: Q1 2019 Cybercrime Tactics and Techniques

Cybercrime is a plague that affects all parts of society – businesses and individuals alike. Yet there are distinctions to be made in the nature of the threat facing different elements of society.

Common criminals, looking to make a fast, illicit buck have historically gone after individuals – via spam, phishing, ransomware and the other tricks of the digital con-man. Businesses have more typically been the target of more sophisticated attacks.

These distinctions have always been blurred somewhat: phishing, for example, is often the first stage of an advanced persistent threat attack or a business email compromise (BEC) scam aimed at a business. And the threat landscape constantly morphs. Over the past couple of years, for instance, we witnessed the focus of ransomware attacks shift from individuals to businesses, as criminals realised the latter have deeper pockets. Then we saw ransomware attacks fall off entirely as other forms of attack, notably BEC, came into vogue.

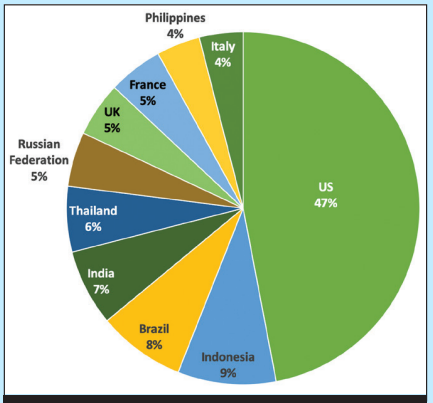
Malwarebytes' latest report, with figures drawn largely from telemetry from its business and consumer security products, shows how this evolution is continuing, with cyber criminals leaning more towards setting their sights on businesses and with two threats being particularly prevalent – the widespread use of the Emotet trojan and a return of the ransomware menace.

"Threat actors are continuing to eye businesses for high returns on investment," says the report in its introduction, "breaching infrastructure, exfiltrating or holding data hostage and abusing weak credentials for continued, targeted monitoring. From a steadfast increase of pervasive trojans, such as Emotet, to a resurgence of ransomware lodged against corporate targets, cyber criminals are going after organisations with a vengeance."

The figures from Malwarebytes show a 195% increase in ransomware detections – that is, attempted attacks – caught by enterprise defensive systems. On the other hand, ransomware targeted at individuals remains at a low level, malware aimed at consumers has dropped by 40% and crypto-mining has all but disappeared. The latter, says the report, is in no small part due to the demise of Coinhive. This was a crypto-mining operation that was employed in a (more or less) legal fashion by websites to use their visitors' CPU cycles to generate crypto-currency. But it was also heavily abused. When Coinhive shut its doors, much illicit crypto-mining went with it.

"There's been a definite shift in the cyber landscape in recent years," says Marie Clutterbuck, CMO at Tectrade. "Cyber criminals have changed their focus from consumers to businesses. Zero-day attacks are on the rise and estimated to be a daily occurrence by 2021. This is largely down to digitisation within organisations and there's more pressure on developers to deliver software faster, leaving systems vulnerable. This problem is exacerbated by hackers becoming more sophisticated, enabling them to bypass defences more easily."

The shift in focus towards business should not come as a surprise, comments Andy Baldwin, VP EMEA at Ivanti. "When it comes to an enterprise business, a threat actor is able steal a larger quantity of data, such as credit card information or health records, or ransom a large number of systems in order to get a higher payout," he says. "A consumer would not be willing to pay much to unransom their system, but a business can easily be convinced to pay £50,000 to recover a large number of systems."



Top 10 countries for malware detections. Source: Malwarebytes Labs.

As cyber criminals change their tactics, so too must enterprises. "IT teams often prioritise stopping a breach occurring at all, but in today's cyber climate a successful breach is inevitable," says Tectrade's Clutterbuck. "The most important aspect of cyber security is that businesses prepare for the worst and have effective data recovery and back-up systems in place. Zero-day recovery makes sure critical systems are down for as little time as possible. It's often true that real damage from these breaches doesn't come from the attack itself, but the resultant downtime after a breach."

Individuals have always presented criminals with an easy target because of a general lack of knowledge about, or investment in, protective measures. Your average computer user probably knows enough about the threat to pay for an anti-malware package, but not enough to keep it, and other software, fully patched. You might think that enterprises would be better protected but that's not always the case.

"The expectation is that large organisations have the resources to implement strong security controls," says Baldwin. "Having the resources, and applying the right priorities for investment in security, unfortunately, are two different things. Project priorities tend to focus on supporting business strategies rather than preventing attacks. And yet a successful cyber attack does a lot more damage than a delayed business SAP implementation, for example. As a result, the cyber criminals are seeing greater potential for success – both in hacking business systems, as well as the rewards associated with this – so they are investing more of their time and efforts into this strategy."

The report is available here: https://go.malwarebytes.com/q1-2019-ct-nt-report-lp.html.

In brief

Israel bombs alleged Hamas hackers

In the first known example of a nation mounting a 'kinetic' response to alleged hacking attacks, aircraft of the Israel Defence Forces (IDF) bombed a building in the Gaza Strip which, it said, housed a Hamas cyber operation. No details were offered about the activities of the Hamas group, but an IDF statement claimed that its own cyber unit, in co-operation with Israel's Shin Bet security service, had successfully repelled a cyber attack from hackers which it said it had traced to the building in the Gaza Strip. Even though the alleged cyber attack was not successful, Israel took the decision to respond with an air strike rather than 'hacking back'. This has raised questions in the international community over the proportionality and legality of the military action. "The scarce official announcement suggests that the potential cyber attack has been thwarted using technical means. That will make analysts wonder what was the point, and justification grounds for using kinetic force," commented Dr Lukasz Olejnik, an independent cyber security, privacy advisor and research associate at the Centre for Technology and Global Affairs, Oxford University.

TA505 targets financial firms

Security firm Cybereason has uncovered a major hacking campaign by a group known as TA505. Believed to be responsible for the information-stealing malware Dridex and the Locky ransomware, TA505 is now engaged in a highly targeted spear-phishing campaign aimed at financial services companies. The attacks are notable for their advanced techniques, which include the use of signed executables and 'living off the land' binaries (LOLBins), which exploit existing, legitimate software present on the target's computer, partly to achieve persistence. The attackers focus on just a few targets within each company, using careful timing to maximise their chance of success. They are also careful to clean up after an attack, including using self-destruct mechanisms to prevent analysis of the malware. The malware is signed and verified by the Sectigo RSA Code Signing Certificate Authority, with this happening just hours before an attack in some cases. There is more information here: http://bit.ly/2DUKMr3.

IoT risks

Research by the Ponemon Institute, sponsored by risk management firm the Santa Fe Group, shows a dramatic increase in data breaches arising from unsecured Internet of Things (IoT) devices. Since 2017, such attacks have increased 26%. A quarter of firms reported a data breach and 24% reported a cyber attack due to an unsecured IoT device or application in the last year, up from 15% and 16% respectively in 2017. And more IoT exploits are being reported at the third-party level: 18% of companies experienced a data breach and 23% experienced a cyber attack caused by a third party's unsecured IoT devices in the last year. And things are not likely to get better any time soon – 87% of respondents said it's likely their own organisations will experience a cyber attack such as a denial of service caused by unsecured IoT devices or applications in the next 24 months, and 84% expect their organisations to experience a data breach for the same reason.

Quick response for US agencies

The US Department of Homeland Security has issued Binding Operational Directive 19-02 which now requires all federal agencies and departments to patch critical vulnerabilities in Internet-exposed systems within 15 days of detection and high-severity flaws within 30 days. This effectively halves the time permitted to fix Internet-facing issues. Actions will be monitored by the Cyber security and Infrastructure Security Agency (CISA). Full details are here: https://cyber.dhs.gov/bod/19-02/.

Trump issues executive order

US President Donald Trump has issued an executive order aimed at improving cyber security co-ordination and training within government and the military. The order directs the Secretary of Homeland Security to create a scheme providing for the rotation of cyber security staff between organisations to help build broader experience and share insights. It also calls for the use of the National Initiative for Cybersecurity Education (NICE) and NIST's Cybersecurity Workforce Framework to gauge the skills of industry practitioners and instructs the Director of the Office of Personnel Management (OPM) to compile a list of cyber security aptitude tests that agencies can use to evaluate practitioners. There will also be an annual competition among agencies. This move comes a year after Trump suddenly, and without explanation, eliminated the position of cyber security co-ordinator, a role established by the Obama administration. The order is here: http://bit.ly/2vHKRcW.

Office 365 takeovers

Account takeovers (ATOs) of Microsoft Office 365 accounts have been used to mount major attacks, according to research by Barracuda. The firm found that around 4,000 accounts that had been compromised within a single month were exploited to launch attacks such as spear-phishing, business email compromise (BEC) and malvertising. Gaining control of accounts involved a combination of "brand impersonation, social engineering and phishing," according to Barracuda's report. The attackers would often impersonate high-profile companies such as Microsoft to convince account owners to visit web pages where they had set up fake login pages. Once they were able to access an account, the hackers would then establish special mail rules to mask their activity. Around a quarter of the IP addresses used during suspicious logins were based in China, with others located in Brazil (9%), Russia (7%), the Netherlands (5%), and Vietnam (5%). There's more information here: http://bit.ly/2Y7w7jC.

Police warn schools

Police forces in Scotland have written to every secondary school in the country warning them that children are increasingly being targeted for recruitment as 'money mules' for cyber criminals. Mules are people used by criminals gangs to 'cash out' – for example, by using cloned payment cards at ATMs to withdraw funds, cashing in gift cards and so on. Cyber criminals have long recruited mules via spam campaigns, social media and – increasingly – WhatsApp messages. They offer easy money for 'working at home', with the mules sometimes not realising they are part of a cybercrime operation. "The fraudsters involved in orchestrating mule accounts are often from serious organised crime groups and any involvement with them can be dangerous," said Detective Inspector Graeme Everest of the Organised Crime and Counter Terrorism Unit (OCCTU). "There are victims affected by fraud across Scotland and this can have a devastating effect on people financially and emotionally. It isn't a victimless crime and by laundering money gained from these victims, you are playing a part in this." Money mules have received sentences of as much as 14 years.

Ethereum brute forcing

Researchers at Independent Security Evaluators (ISE) have discovered that it's possible to brute force private keys being used for the Ethereum blockchain, and that this is facilitating theft of the crypto-currency. ISE was able to identify 732 actively used private keys as a result of poor key generation practices by Ethereum users. It also noted that 13,319 Ether (ETH) was transferred to invalid destination addresses (and thus lost forever) as well as to wallets derived from weak private keys which were targeted for theft. This represents a loss of $18.9m at peak prices for the crypto-currency. There's more information here: http://bit.ly/2V2HLKU.

People cause cloud breaches

Nine out of 10 data breaches involving cloud services are caused by people, not issues with the platform or technology, according to new research by Kaspersky Lab. While organisations place a lot of attention on ensuring that cloud services assume responsibility for the security of data on their services, data breaches mostly occur as a result of social engineering attacks against the organisations' own staff. This is true in 88% of cases with smaller firms and 91% of cases involving enterprises. The report is here: http://bit.ly/2VmGALm.

How readable are data breach notifications?

Stephen Jackson, University of London

Stephen Jackson

Data breaches – broadly defined as incidents where protected data that is considered sensitive and confidential has been disclosed, accessed and/or altered in an unauthorised manner – present a growing threat to society and organisations. While much of the focus to date has been on technical countermeasures, particularly the ways to prevent and detect security threats associated with data breach incidents, we also need greater insights into the readability of the notification response used by firms to alert affected consumers after a suspected incident has taken place.

The proliferation of data breaches has led to the creation of mandatory data breach notification laws. The need for mandatory data breach notification was first introduced by the state of California back in 2002 (enacted 2003). This was largely in response to the growing number of data breaches putting consumers' personal and sensitive information at risk from hackers, accidental loss or misplacement.

Since 2018, all US states have endorsed legislation requiring private and government entities to notify individuals who may be victims of a data breach involving their personal information.[1] Emerging from the US, mandatory data breach notification laws have spread worldwide, including, for example, Australia, Canada, South Korea, Philippines and European countries, among others. Interestingly, as a result of strict notification regulations, as well as being enforced across all states, US firms amass the highest data breach notification costs at £740,000.[2]

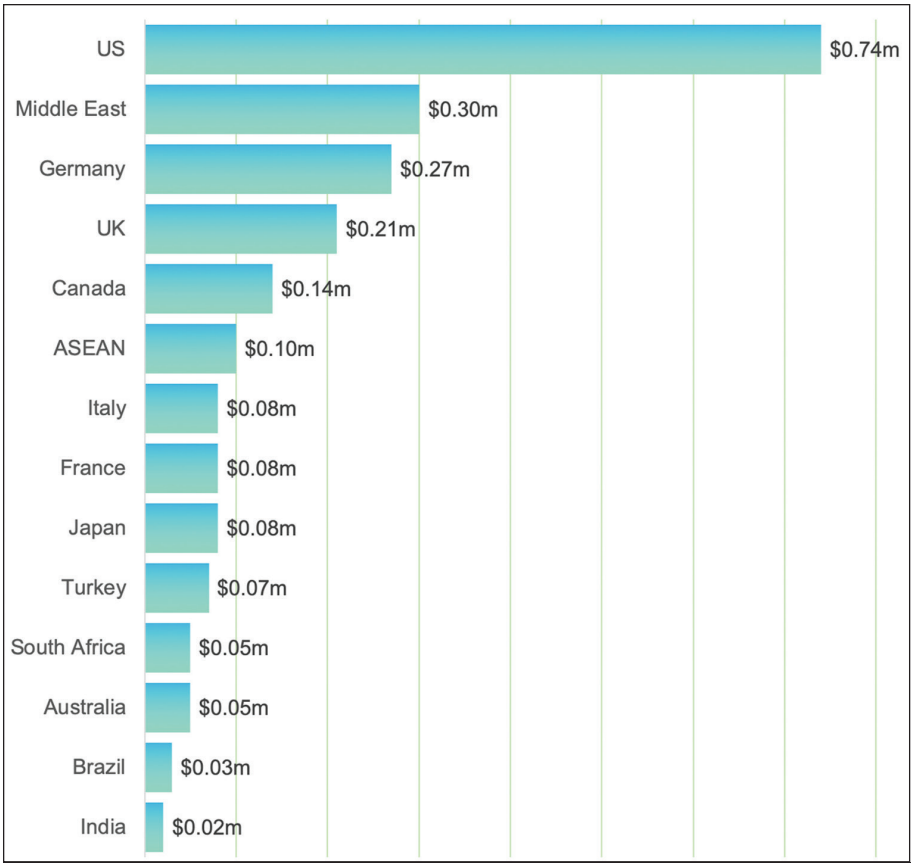


Figure 1: Data breach notification costs, in US$ millions. The Middle East includes the UAE and Saudi Arabia. ASEAN includes Singapore, Indonesia, Philippines and Malaysia. Source: Ponemon Institute.

While laws can differ between and even within countries, companies are typically required to notify consumers, usually in writing, if they have been subjected to a data breach. Often the purpose of these laws is to ensure that firms provide consumers with accurate and timely information concerning the incident, with much advice recommending that notifications should be written in a clear manner which, one would expect, are easy for consumers to read. This raises an interesting question: how readable are data breach notifications? Before attempting to answer this question, let's briefly examine the concept of readability.

Readability

Readability is concerned with how difficult it is for one to understand a message in relation to the writing style.[3,4] In order for a message to be comprehensible, it must be written (encoded) in a way which is easy for individuals to understand at the moment of decoding.[5,6] If the message is offered in a manner that is overly convoluted and exceeds the capacity of the reader to grasp, the consequences can be a restriction in the decision-making capabilities of the intended readers or poor knowledge absorption.[7] In assessing reading difficulty, a common approach is to use a readability formula.

For this study, the Flesch Reading Ease test was used. The Flesch test is among the most common methods for assessing the readability of a passage in English.

Drawing on two core measures (word length and sentence length), Flesch assesses how difficult a passage in English is to read.[8] To calculate the Flesch score, the Advanced Text Analyser tool from the website UsingEnglish.com (which provides advanced readability resources and tools for researchers) was utilised. The use of a computerised tool to calculate the Flesch score was chosen as this method is deemed to be more precise and consistent than by manual calculation.[9]

The formula to calculate the Flesch Reading Ease is:

$$206.835 - 1.015\left(\frac{total\ words}{total\ sentences}\right) - 84.6\left(\frac{total\ syllables}{total\ words}\right)$$

For the Flesh Reading Ease test, the higher the reading ease score, the easier it is to read the text. Alternatively, the lower the reading ease score, the more difficult it is to read the text.

Analysing results

As part of an investigation examining the readability of data breach notifications to consumers following a data breach incident, 521 US notification letters across various sectors, including education, finance, healthcare, retail, service, technology and travel/hospitality, were analysed. Since US firms encounter the highest notification costs and data breach notifications can be easily accessed from Attorney General websites, it was decided to focus on that country.

Thirty-four out of 521 data breaches were associated with public firms and the average firm size consisted of 200-1,000 employees. The results reveal the mean Flesch Reading Ease score to be 45, with results falling within the range 30 (very difficult/difficult) to 71 (fairly easy). Although much guidance advises that notification should be written in a manner that is clear and straightforward, these results indicate that the majority of firms use a writing style that is difficult to read.

To put the results into perspective, the recommended readability in terms of typical education level is grades 7-8,

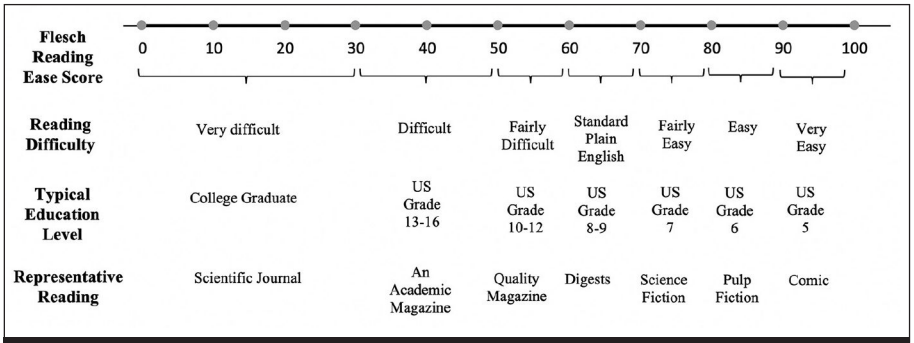


Figure 2: Flesch Reading Ease interpretation.

with guidance advising that businesses should strive for grade 8 to enable the message to be read by 80% of the US population.[10,11] In a separate study, which examined the readability of data breach notifications in conjunction with firm characteristics and the severity of the data breach incident, the findings revealed that the greater the data breach severity, the higher the reading complexity of the breach notification becomes.[12]

More severe data breach incidents were associated with higher financial, reputational and legal costs, as well as long-term organisational impact. In addition, the results revealed that privately owned firms were more inclined to craft less-complex data breach notification responses, and there was a tendency for larger firms to produce letters that consist of fewer words, fewer unique words, and slightly longer words.

Interpreting the results

This raises an important question: why do business managers write in more complex ways when crafting data breach notification responses? As a way of addressing this question and interpreting the results, three possible explanations drawn from the readability literature are considered: a) bad writing; b) information assumption; and c) impression management.

Rather than assuming that complex writing practices are a product of deliberate manipulation whereby managers intentionally set out to write in a convoluted manner, reading difficulty can be the product of bad writing practices through the use of overly complex words. While there can be many explanations for bad writing in the workplace, in the context of data breach incidents, some of the key reasons may be lack of knowledge about the causes and/or outcomes of the data breach incident, inadequate resource provision or dearth of experience in communicating data security issues.

A second possible explanation, referred to here as the information assumption, is that data breach incidents may be difficult to describe, thus requiring more complex words – or those crafting the response believe that those affected by the incident will require (and demand) more complex writing and terminology. Managers may deliberately increase the complexity of their vocabulary so as to reassure consumers that the business managers know what they are talking about.

A third explanation for the results relates to impression management. As data breaches can be a form of negative news for organisations, it is important that those disclosing the data breach attempt to frame the communication in a way that makes the firm look as good as possible.[13] Consequently, it may be the case that firms are deliberately manipulating the information by making the writing more difficult as a way of masking the implications of the situation, distracting the reader from the significance of the event and discouraging them from reading further.[14]

If impression management is at play, why would organisational managers, in the case of data breaches, want to engage in these types of behaviours or tactics? In the US, for example, unlike other types of security vulnerabilities – which, from a regulatory perspective, do not always have

to be reported – companies have a legal obligation to follow specific actions when responding to and reporting data breaches.[15] Since data breach incidents are in the public eye, it may be the case that managers are more inclined to engage in impression management compared to other IT security incidents. As a firm's performance can be associated with financial incentives (eg, cash bonuses, remuneration packages, tenure, salary), managers may have a financial incentive to make the reading difficult as a way to protect their reputation, prospects and compensation and/or maximise material outcomes.

Implications

If mandatory data breach notification letters are being drafted in ways that are too complex, this runs the risk of undermining the quality and purpose of such notifications. More specifically, consumers, as members of society, may not be effectively informed of the facts pertaining to the data breach incident, as well as the inability to take appropriate and effective remedial measures.

Furthermore, consumers may need to take more time to read and fully understand the data breach notification, particularly the impact that the breach will have on their personal data and the actions they may need to take. It may be useful for business managers and regulators to develop better policies and clearer incident response mechanisms by promoting educational programs re what data breach notifications should be comprised of.

The Flesch readability test, among other readability measures, is a useful starting point for gauging the reading complexity of a piece of text. What might be surprising is that readability measures, including the Flesch test, are often part of common word processing packages. Readability scores can provide writers with useful information regarding how complex the message is for the intended audience, and if necessary, allow them to redraft the response in a more straightforward manner.

Merely providing additional information relating to the disclosure will not improve the overall communication. Instead, improvements to the readability are needed to increase the clarity and transparency of the disclosure communication.

About the author

Stephen Jackson is a senior lecturer in technology and information management at Royal Holloway, University of London. Prior to joining academia, he worked in the area of computer forensics for a 'big four' accounting firm on a variety of assignments across various sectors in Europe and Asia. His current research interests include data breaches, information security and the management of IT projects. He can be reached at Stephen.Jackson@rhul.ac.uk.

References

1. 'Brown Rudnick alert: All US states now require breach notification and more mandate cyber security measures'. Monodovisione, 10 Apr 2018. Accessed Feb 2019. www.monodovisione.com/media-and-resources/news/brown-rudnick-alert-all-us-states-now-require-breach-notification-and-more-ma/.
2. '2018 Cost of a data breach study: Global overview'. Ponemon Institute, Jul 2018. Accessed Feb 2019. https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf.
3. Klare, G. 'The measurement of readability'. The Iowa State University Press, Ames, Iowa, 1963.
4. Pound, GD. 'A note on audit report readability'. Accounting and Finance, Vol.21, Issue 1, 1981, pp.45-55.
5. Bayerlein, L; Davidson, P. 'The influence of connotation on readability and obfuscation in Australian chairman addresses'. Managerial Auditing Journal, Vol.27, Issue 2, 2011, pp.175-198.
6. Hall, S. 'Encoding/decoding'. In Hall, Hobson, Lowe & Willis, 'Culture, media and language: Working papers in cultural studies', 1972-1979 (pp.128-138). Hutchinson, 1980.
7. Courtis, J. 'Readability of annual reports: Western versus Asian evidence'. Accounting, Auditing and Accountability Journal, Vol.8, Issue 2, 1995, pp.4-17.
8. Flesch, R. 'A new readability yardstick'. Journal of Applied Psychology, Vol. 23, 1948, 221 – 233.
9. Bakar, AS; Ameer, A. 'Readability of Corporate Social Responsibility Communication in Malaysia'. Corporate Social Responsibility and Environmental Management, Vol.18, Issue 1, 2011, pp.50-60.
10. Casola, C. 'Content, readability, and understandability of dense breast notifications by state'. The Journal of the American Medical Association, Vol.315, Issue 16, pp.1786-1788.
11. Colmer, R. 'The Flesch reading ease and Flesch-Kincaid grade level'. Readable. Accessed Feb 2019. https://readable.com/blog/the-flesch-reading-ease-and-flesch-kincaid-grade-level/.
12. Jackson, S; Vanteeva, N; Fearon, C. 'An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: Evidence from US firms'. Journal of the Association for Information Science and Technology. In Press.
13. Veltsos, J. 'An analysis of data breach notifications as negative news.' Business and Professional Communication Quarterly, Vol.75, Issue 2, 2012, pp.192-207.
14. Courtis, J. 'Annual report readability variability: Tests of the obfuscation hypothesis'. Accounting, Auditing & Accountability Journal, Vol.11, Issue 4, 1998, pp.459-472.
15. Brew, K. 'What's the difference between a data breach and a security incident?' AlienVault, 30 Dec 2014. Accessed Feb 2019. www.alienvault.com/blogs/security-essentials/whats-the-difference-between-a-data-breach-and-a-security-incident.

Gamification as a winning cyber security strategy


Brad Wolfenden

Brad Wolfenden, Circadence

We are more connected than ever before. Our smart TVs and refrigerators, phones and drones, online bank accounts and electronic health records, and so much more, are on the web and in the cloud – connected and 'talking' to each other. While creating convenience for the end user, this growing interconnected digital footprint creates a ripe surface for a cyber criminal to attack.

Why? The more devices we connect to each other, the more difficult it becomes to attribute where a threat is coming from, not to mention the increased number of entry points for exploitation.[1] And that means the bad guys are more likely to get away with their attack before defenders even know what's happening. Just like in some video games, consumers and business leaders find themselves battling the consequences of interconnectivity and are trying to keep the opponent from exploiting their information and damaging their reputation. In this 'game of protection' to balance defensive and offensive security techniques, now is the time for CISOs and business leaders to reach for a new cyber security manual – one that leverages gamification.

Gamification, a popular buzzword in the technology sphere, is now gaining momentum as a learning strategy both in academia and across the enterprise for professional development. It's commonly defined as a process of adding game-like elements to something. In short, gamification integrates aspects of gaming – eg, chat boxes, leaderboards, levelling up, unlocking badges, etc – into real-world, virtual environments.

The term was originally coined in 2002 by British computer programmer Nick Pelling and hit the mainstream when a location-sharing service called Foursquare emerged in 2009 (at Austin, Texas' SXSW, no less), offering gamification elements such as points, badges and 'mayorships' to motivate people to use their mobile app to 'check in' to places they visited. The term hit buzzword fame in 2011 when Gartner officially added it to its Hype Cycle list.[2]

Hands-on activity

But gamification is more than just adding gaming elements to an environment or scenario. It is adding those elements in ways that prompt our human desires to socialise, achieve, and master and build skills and status. Think about your favourite game. Maybe it is a board or card game, sport or even a computer or video game. Why can't you stop playing it? Because you are rewarded in some way for 'good' actions and that makes you feel notable. This kind of positive reinforcement motivates humans and offers tangible – often immediate – evidence of our progress.

"Cyber challenges, code sprints and other gamified activities and competitions hold enormous promise in both the public and private sectors and can be used in all phases of the employment lifecycle"

New learning methods are now more important than ever. The 21st Century has introduced five generations (ie, Gen Z, Millennials, Gen X, Baby Boomers, the Greatest Generation) into the workforce, with shifts being experienced in the employer-employee dynamic. Gamified activity is hands-on activity and it taps into the 'learn by doing' approach that is the natural way humans learn even the most basic of skills, such as walking, using a keyboard, driving a car, cooking etc.

The next generation of cyber professionals is also the first digitally native generation. Beyond video games, these people have been raised with educational smart apps, classroom smart boards and shared Google Docs. It is second nature for them to socialise as they play and as they learn, and to broadcast their achievements on social platforms, gathering informal 'likes' and sharing formal 'certs' to validate their efforts.

These activities allow employers to create ways to make learning, team building and skill-proving cyber security fun. Cyber challenges, code sprints and other gamified activities and competitions hold enormous promise in both the public and private sectors and can be used in all phases of the employment lifecycle. This includes supporting organisational needs for candidate supply, assessing skills with a more engaging candidate experience, as well as from a career development strategy to upskill existing talent.

It isn't all about Gen Z though; learn-by-doing models are advantageous to professionals of all generations, from millennials to mid-career workers because gamification is more than the new, shiny object on the heels of artificial intelligence and machine learning. As a learning strategy, gamification is proving its effectiveness both for knowledge retention and for encouraging

re-engagement of perishable skills, making them more 'sticky' – two critical necessities for cyber teams in the wake of imminent and evolving cyberthreats.

Cyber ranges

In cyber security, gamification can manifest within cyber ranges – that is, virtual environments that provide simulations of real-world networks, systems and tools for professionals to safely test and train in a closed environment that does not compromise the stability and security of production networks.[3] The National Initiative for Cyber Security Education reports that ranges provide:

- Performance-based learning and assessment.
- A simulated environment where teams can work together to improve teamwork and capabilities.
- Real-time feedback.
- Simulated on-the-job experience.
- An environment where new ideas can be tested and teams work to solve complex cyber problems.

Cyber ranges were initially developed for government entities looking to better train their workforce with new skills and techniques. Today, cyber ranges are known to effectively train the cyber workforce across industries from healthcare to government or financial institutions. Individuals and teams can participate in a virtual environment at any time, creating comfortable social settings that allow them to practise and master skills, collaborate in team-based challenges and compete for leaderboard status in friendly situations. Users can apply what they know within the simulated environments or 'worlds', creating a natural flow that keeps them engaged and focused. The outcome is highly skilled and educated professionals who have better understandings of cyber best practices and can effectively apply learned knowledge to real-world situations.

As technology advances, ranges gain in their training scope and potential. Today, ranges are still primarily used as a 'train as you would fight' tool but businesses are finding other complementary uses for them as well, including hiring and retaining talent and promoting general security awareness.

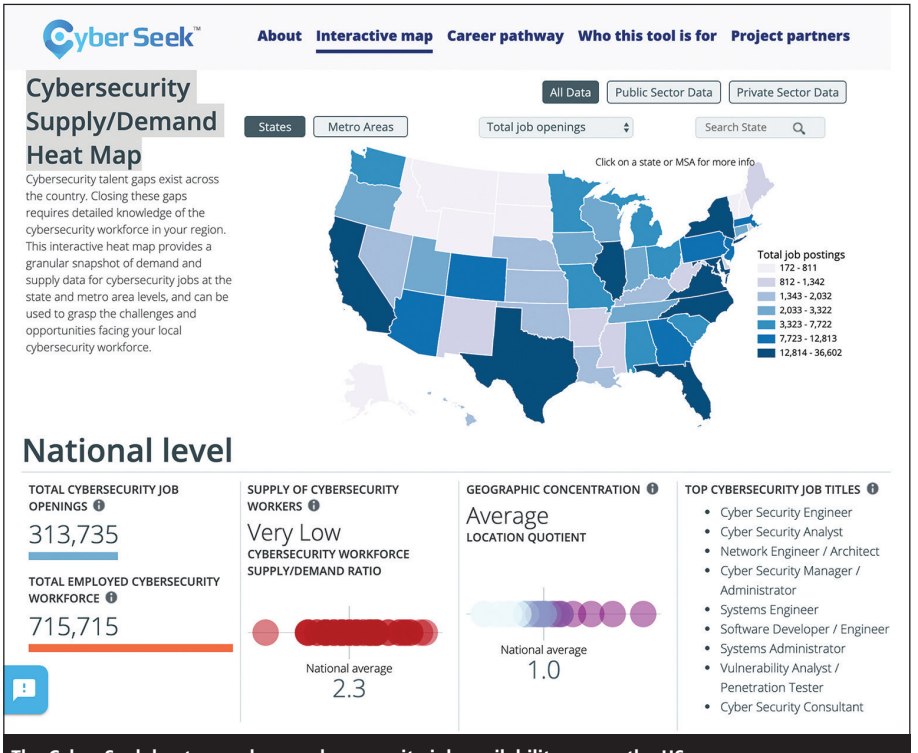
Skills gap

Gamified cyber ranges can be used to recruit and assess incoming and prospective talent. This is important given the widening cyber skills gap the industry faces today. Currently there are over 300,000 open cyber positions across the US, according to CyberSeek.[4] Recruiters can start filling these positions using gamification to compare prospective employees' listed credentials on their resumé to what they actually know and apply in a real-life situation. This method can help hiring managers hire new talent with confidence and better evaluate their contributions to the workplace.

In addition, gamified cyber ranges can be used to raise general security awareness among staff. One does not need to have a technical certification or extensive background in cyber to engage on a range. Non-technical professionals are using ranges to educate themselves on security best practices and policies such as what a suspicious email looks like, how to tell if you are receiving a phishing email, or unintentionally installing malware, etc.

"Non-technical professionals are using ranges to educate themselves on security best practices and policies such as what a suspicious email looks like, how to tell if you are receiving a phishing email, or unintentionally installing malware, etc"

Humans are the weakest point in any security strategy. According to the '2018 Cost of Data Breach' study by the Ponemon Institute, 25% of data breaches in the US were triggered by human error, including failure to properly delete data from devices.[5] This is why gamification in cyber security is not only necessary but is an exciting way to engage all types of professionals in an important issue that impacts us all, from back-end tech developers to end-users.



The Cyber Seek heat map shows cyber security job availability across the US.

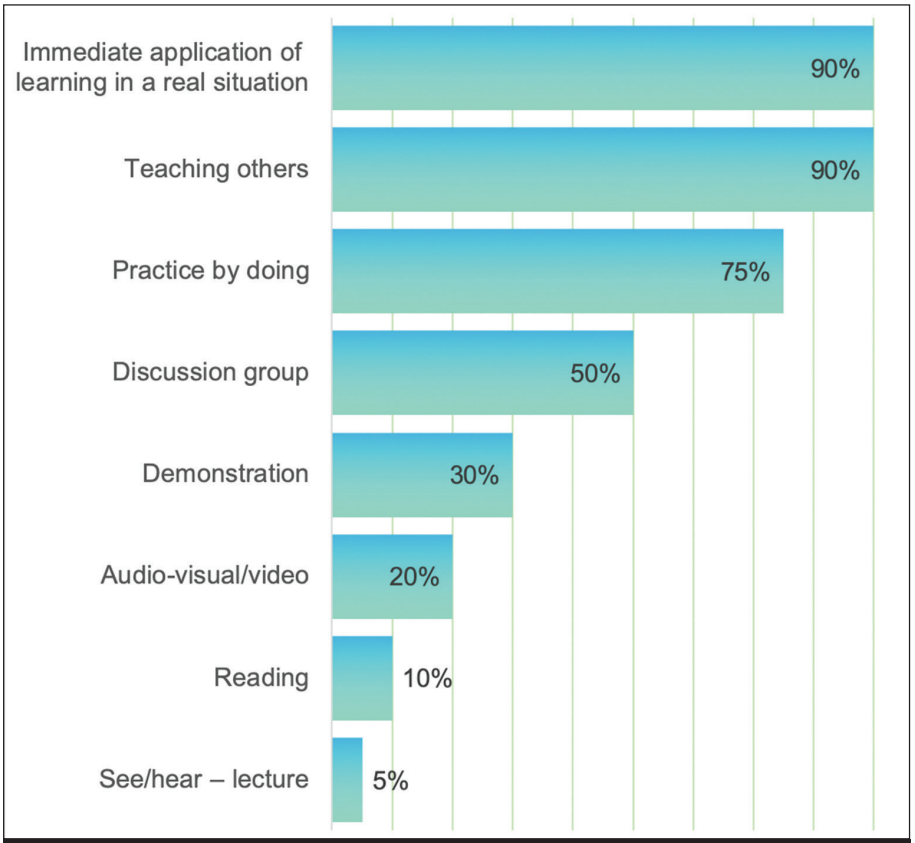
Cyber learning outcomes

The use of gamification in cyber learning is breaking ground as research and real-time results demonstrate its usefulness in hardening company cyber preparedness efforts. Hands-on activity puts learned knowledge to the test so that instructors and managers can identify gaps in performance and find ways to continuously improve – helping professionals do their jobs better and more efficiently. Additionally, the learn-by-doing approach helps users apply concepts to real-world exercises and scenarios, improving information retention rates to 75% compared to 5% through more lecture-based, passive-learning methods.[6]

Increasing information retention is critical for cyber security departments because there is a monetary cost associated with training professionals as well as the related potential costs associated with attacks that get past ill-equipped security teams. The cost of traditional offsite cyber courses can carry a high price tag when you factor in travel and course materials as well as the impact of time away from the defensive frontlines. PowerPoint and 'click-fest' learning models often fail to truly engage students – they hear the concepts, retain a subset of the learning, but struggle to put the material into practice once back in the office.

"A workforce that is dedicated to continuous learning demonstrates a spirit of problem-solving, exploration and discovery vital to cyber security work"

In short, management are not truly getting the most ROI bang for their buck. These applied learning limitations are critical because according to an ESG/ISSA study, 70% of cyber security professionals claim their organisation is impacted by the industry skills shortage.[7] Ramifications include an increasing staff workload, hiring and training junior personnel rather than experienced professionals, employee retention, and situations where teams spend most of their time dealing with the emergency *du jour*, rather than proactive planning.



Knowledge retention rates for different teaching methods. Source: Play to Teach.

When you think about the next evolution of cyber security readiness, gamification makes perfect sense.

- Game-like environments are more engaging than sitting and watching a lecture-based presentation.
- Completing realistic exercises on company emulated networks with teammates promotes strategic problem-solving.
- Continuous learning hones skills in ways traditional courses cannot offer.

Gamification brings more to the table. Gamified learning environments also provide a safe space for trial and error, enabling cyber professionals to explore new techniques and think outside the box. Both outcomes are extremely important to professionals' ability to think on their feet and react quickly but strategically to new threats and attacks.

In conclusion

What we need now are open minds: minds that embrace the power of people to drive better security solutions; that understand today's cyber skills shortage demands automated and augmented approaches to job efficiency; and that know how to beat the hackers at their own game. With gamification and through gamified learning we can evolve the industry for the better. A workforce that is dedicated to continuous learning demonstrates a spirit of problem-solving, exploration and discovery vital to cyber security work.

In today's interconnected business world, made more vulnerable with every new connection and sync, we have a lot to be fearful about – but we also have a lot to be excited about. Unique innovations, advances in artificial intelligence and machine learning and gamification are paving new pathways for security professionals to win the cyber security 'game'. It is a pathway, a playbook, an approach that is sustainable, persistent

and proactive. When it comes to playing the game of protection, every second of increased information retention, skills application, badge rewards and problem-solving matters.

About the author

Brad Wolfenden is the director of cyber academic partnerships for Circadence and a technology leader in cyber security education, learning and assessment. He has built a successful portfolio of academic partners using a gamified cyber learning platform to drive increased awareness, engagement opportunities and dynamic, virtual learning environments to computer science and cyber security students at all proficiency levels. Ranging from K-12 to post-graduate programming, Wolfenden has designed, delivered and managed industry-academic-government partnerships focused on computer science and cyber security. He is a member of the NICE Working Group, the NICE Collegiate, Competitions, and K12 Subgroups, and member of the Microsoft Education Partnership Advisory Council.

References

1. 'The Internet of Things will cause more security problems next year, exec warns'. CNBC, 29 Nov 2018. Accessed Apr 2019. www.cnbc.com/2018/11/29/Internet-of-things-will-cause-security-problems-next-year-says-exec.html.
2. Chandran, Kavita. 'Hype Cycle for Education, 2017'. Gartner, 24 Jul 2017. Accessed Apr 2019. www.gartner.com/en/documents/3769145.
3. 'Modernising Cyber Ranges'. Circadence, 13 Nov 2018. Accessed Apr 2019. www.circadence.com/about/circ-blog/modern-cyber-ranges/.
4. 'Cyber security Supply/Demand Heat Map'. Cyber Seek. Accessed Apr 2019. www.cyberseek.org/heat-map.html.
5. '2018 Cost of a Data Breach Study'. Ponemon Institute/IBM. Accessed Apr 2019. www.ibm.com/security/data-breach.
6. 'Solving the training dilemma with game-based learning'. Play to Teach. Accessed Apr 2019. https://cdns3.trainingindustry.com/media/3203537/game based learning.pdf.
7. 'The life and times of cyber security professionals'. ESG/ISSA. Accessed Apr 2019. www.esg-global.com/esg-issa-research-report-2017.

IoT security: could careless talk cost livelihoods?


Marc Sollars

Marc Sollars, Teneo

The rise of the Internet of Things (IoT) promises exciting capabilities for business but could it usher in risks that are difficult to assess, let alone deal with? In a world where companies can use Alexa to help set up new office IT, could unsecured IoT systems be the equivalent of careless talk giving away company secrets – and endangering livelihoods?

IoT-based advances such as real-time control of utilities' supervisory control and data acquisition (SCADA) systems, brands boosting customer service with machine learning and property firms providing personalised climates for offices, show the exciting, innovation-shaping capabilities of these technologies. But if IoT systems – and the teams developing them – aren't brought into an overarching data and network security strategy, these technologies could become a weak link in big companies' defences.

Demand for IoT is skyrocketing: Gartner forecasts that worldwide IoT spending will hit $1.5bn in 2018, up 28% on 2017. But risks are growing too: Symantec reported a 600% increase in IoT device attacks in 2017 while the US Family Online Safety Institute's research found that three in 10 parents had children potentially using Internet-enabled toys that share data: the potential for privacy breaches from poorly-secured IoT products is huge.[1,2]

The nub of these problems is that IoT-enabled devices behind cutting-edge consumer and business products must talk securely to the company's core IT and business systems. Without this 'secure conversation', IoT's learning capabilities could simply enable hackers to carry out wider-scale attacks. The problem is only exacerbated by companies' complex network infrastructures and surging data volumes in our online world.

Planning IoT security

Given this bewildering picture, how should in-house operational, network infrastructure and data security teams mitigate IoT risks? Can in-house personnel realistically run expanded security and

network monitoring models? For all these reasons, IoT security presents a formidable challenge.

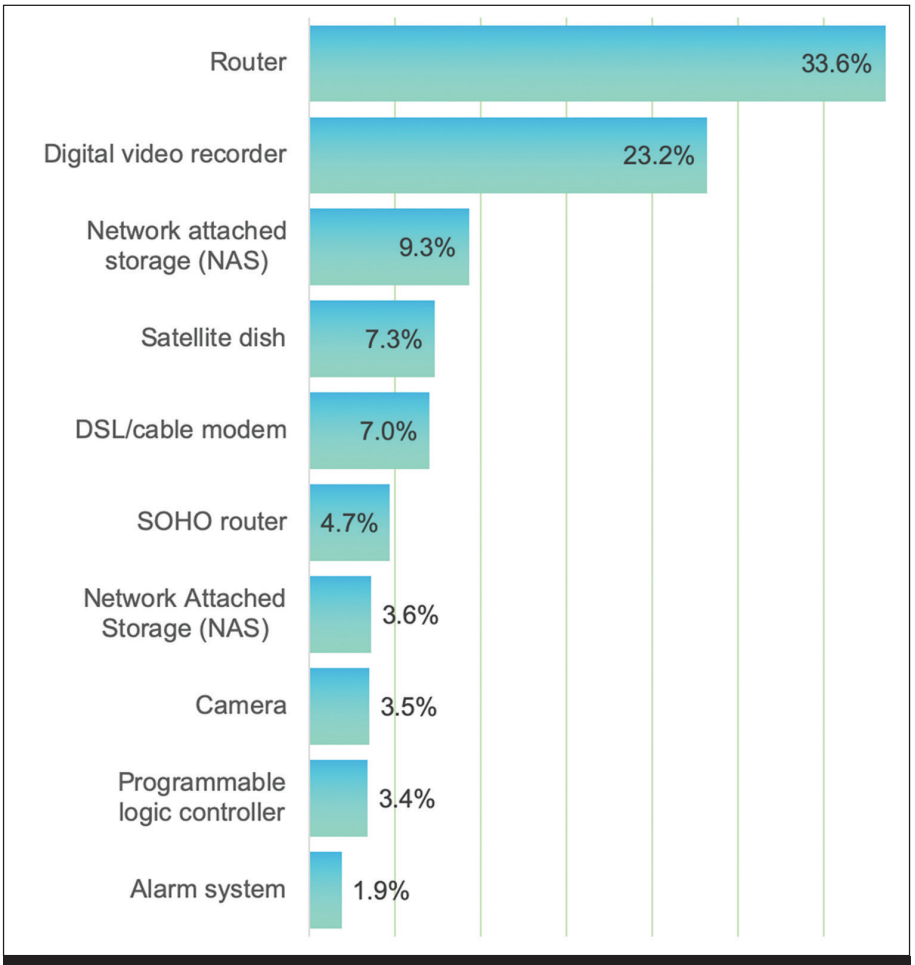
Addressing IoT system risks and dealing with them depends on companies developing regular risk analysis; bringing internal and external teams into IoT security planning; operating company-wide security policies; protecting network endpoints and segmenting networks; generally achieving far better awareness of what is going on in their corporate IT networks; and engineering enhanced network control and automation in the future.

Assessing the risk

Next-generation security begins with IT and security teams modelling 'what if' risk scenarios. These need to assess if the IT or IoT development team has put the latest protection on systems and IoT devices and if the various networks are segmented. How and how quickly can internal teams identify potential issues from different categories of traffic on their networks? Securing IoT means making a step change in understanding how individual components communicate with back-end IT systems and getting sufficient network visibility to plan better risk mitigation and security policies.

"There are readily available tools such as open source network traffic analysers being used for live event monitoring or as flexible analytical platforms for network performance measurement and trouble-shooting"

Another factor is commercial pressure on companies to cut process costs and speed up time to market. It's likely that under-pressure in-house IT and security teams have quietly tried to fix security after a product's launch. Organisations must stay one step ahead of consumers and potential attackers to safely develop next-stage products and services – without their products or reputation being compromised.



The types of Internet of Things (IoT) devices seen performing attacks against Symantec's honeypot systems. Source: Symantec.

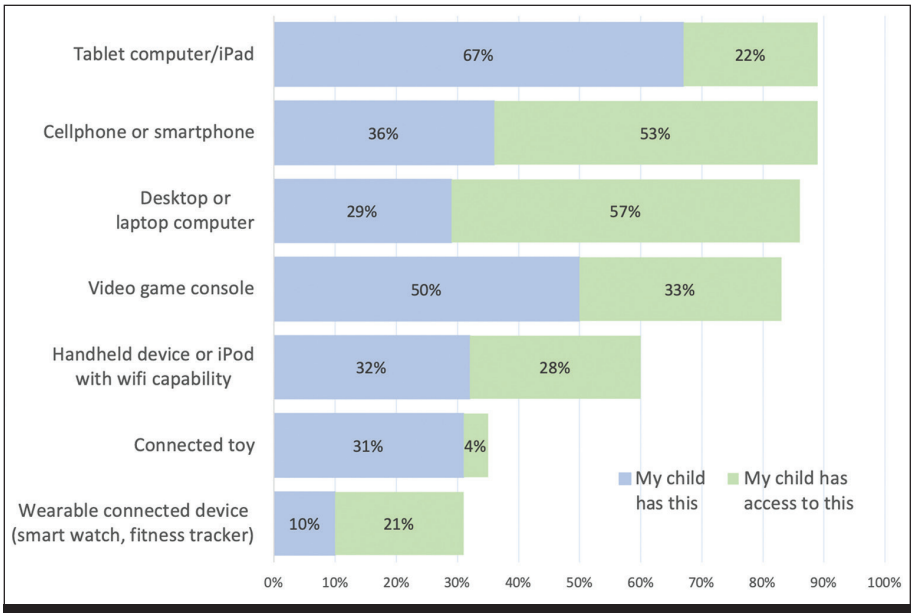
The risks from failing to bring IoT into corporate security strategy are becoming clear. In a recent test, a children's toy could be hacked and used to track children's movements and listen remotely. Incidents like this could potentially sink a brand's reputation or lead to consequential losses from lawsuits.

IoT security and the advanced analytics required have to be embedded in a company's new product development (NPD) – and be robust enough to withstand commercial pressures and potential threats – from the start. These solutions must also be integrated with that under-realised challenge – getting a grip on today's complex global networking infrastructures.

Organising network security, especially analysing the data generated to help evolve security policies, is a big task given the explosion in networks and cloud services. Company WANs not only reach from enterprises to the cloud but also across cloud regions and different vendors. Increased mobile working also means more branch office and individual endpoint connections. And ever-wider connectivity options – such as MPLS, public Internet and 4G – also have to be managed for optimum performance and security. With business data increasingly moving to the cloud, innovative companies will need fresh network insights if they are to fully grasp how their IoT systems communicate across the cloud and see how their security can be hardened.

In-depth security

The overall task for global companies running global networks and cloud operations is naturally to defend in depth – based on network segmentation,



Responses from parents of children aged 12 and younger. Source: Family Online Safety Institute.

employee access controls, reducing or controlling the level of remote access, strong password policies, use of encryption and separating sensitive networks and using trusted and audited third-party contractors.

"With business data increasingly moving to the cloud, innovative companies will need fresh network insights if they are to fully grasp how their IoT systems communicate across the cloud and see how their security can be hardened"

But the real difference in effective security is being made in the crucial *second* part of the security task. This is when all that data arrives at the back end and IT teams try to understand whether hackers or criminals are piggybacking on that traffic – using logs, packet capture and meta traffic – to access core business or IoT systems. But this second stage inevitably creates monitoring and analytics workloads that are often beyond the capabilities – and the budgets – of many internal IT and networking teams.

And as savvy enterprise IT teams demand more visibility of data and network traffic to assist this task, it's third-party networking and analytics experts that are giving corporate customers the extra resources and new insights to cope with this workload. Specialists will find gaps in the customer's networks and IoT set-up and identify solutions to harden the security all the way to the datacentre or the cloud: they give in-house teams the tools to get the IoT security job done.

As a result, we are already seeing global companies partnering with security vendors to protect IoT developments in their industrial platforms. There are readily available tools such as open source network traffic analysers being used for live event monitoring or as flexible analytical platforms for network performance measurement and trouble-shooting. These innovations give hard-pressed internal teams new options such as smarter post-processing or the use of alternative back-ends such as external databases for making added security checks.

As levels of incoming system and security data only increase, IT and security teams can bring in the people and systems to segment traffic and the corporate network fabric to ensure that the right data goes to the right place. As a result, corporate IT and security gain fuller visibility of traffic, events and suspicious behaviour on core and IoT networks and devices to feed into their security plans.

Enforcing policies

Companies are highly motivated with regards to security following high-profile hacks and the arrival of the General Data Protection Regulation (GDPR). But a lasting barrier to locking down IoT is the lack of understanding and co-operation between internal NPD, IT and security teams.

As IoT is widely adopted, organisations need closer co-operation between operational technology professionals (dealing with IoT devices as part of NPD) and IT and infrastructure teams (handling network infrastructure monitoring and optimisation) and security teams driving overall strategy and enforcement. *Ad hoc* thinking, such as NPD plugging gaps revealed by penetration tests, has to give way to co-ordinated company-wide policies.

While internal collaboration is improving, companies need to organise wider education and training on responsibilities for all internal teams, taking account of business goals, corporate and IoT security needs, desired solutions and analytics resourcing plans. IoT security demands that everyone pulls in the same direction.

Network segmentation

It's fundamental to securing IoT that enterprise networks and devices should not meet, since this creates many opportunities for unauthorised access of core networks using sensors and devices. Working with outside experts in network traffic segmentation, IT teams can define relevant controls, so that only desired traffic passes between systems or traffic takes only defined paths between zones.

In-house teams that enlist external specialists can better assess their networking landscapes and desired traffic flows and draw up enhanced segmentation policies. As well as supporting IoT security planning, this joint approach also reduces companies' industry and legal compliance workloads.

Anticipating risks

Global businesses will always need to continual review their security posture and policies and drive enforcement. Can any IT or security team ever say that they have done enough without asking for outside help or more budget? For example, a business services company that has implemented firewalls and enabled endpoint security may struggle with the details of segmentation before it can take steps to achieving better IoT protection. There is a broad comparison with GDPR here: companies cannot develop perfect solutions but they can take practical steps and selectively use outside specialists to help ensure workable security systems.

And looking ahead, how do enterprises investing heavily in NPD and IoT strategies simplify their security planning? An important opportunity is coming with the growing use of software-defined wide area networks (SD-WAN) to put control layers over companies' different networks and components. This advance will bring benefits like IT teams better controlling WANs from a central point, clearer pictures of network issues and intelligent routing of traffic across networks. SD-WAN could enable companies to re-architect legacy networks and potentially gain greater insights into business applications and potential threats to them as the backdrop to long-term IoT development.

Companies excited by IoT's real-time capabilities need to ensure that their security is 'next generation' too. While investing in IoT innovations, enterprises need to enlist external analytics and security expertise to mitigate risks and realise their exciting commercial opportunity.

About the author

Marc Sollars is CTO of Teneo, a specialist integrator of next-generation technology. He is chief evangelist and plays a key role in identifying technologies that are early to market and can be integrated into the company's services portfolio. Sollars is on Twitter at @MarcatTeneo.

References

1. 'Internet Security Threat Report: Volume 23'. Symantec. Accessed Apr 2019. www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.
2. 'Connected Families: how parents think & feel about wearables, toys, and the Internet of Things'. Family Online Safety Institute. Accessed Apr 2019. www.fosi.org/policy-research/connected-families/.

How ethical hacking can protect organisations from a greater threat

Scott Nicholson

By Scott Nicholson, director, Bridewell Consulting

As digital technologies are becoming embedded in all aspects of life, cyber attacks can come from many directions. A significant proportion of these attacks pose serious risks to critical data, infrastructure and processes within all manner of organisations, both large and small.

The World Economic Forum (WEF) now regards cybercrime as one of the biggest threats to businesses and the economy, as noted in its 2019 Global Risk Report.[1] And it's no longer just large enterprises that are at risk. Hiscox estimates that small businesses alone are the target of 65,000 cyber attacks every day, which leads to a successful hack every 19 seconds and an average clean-up cost of £25,700 per year.[2]

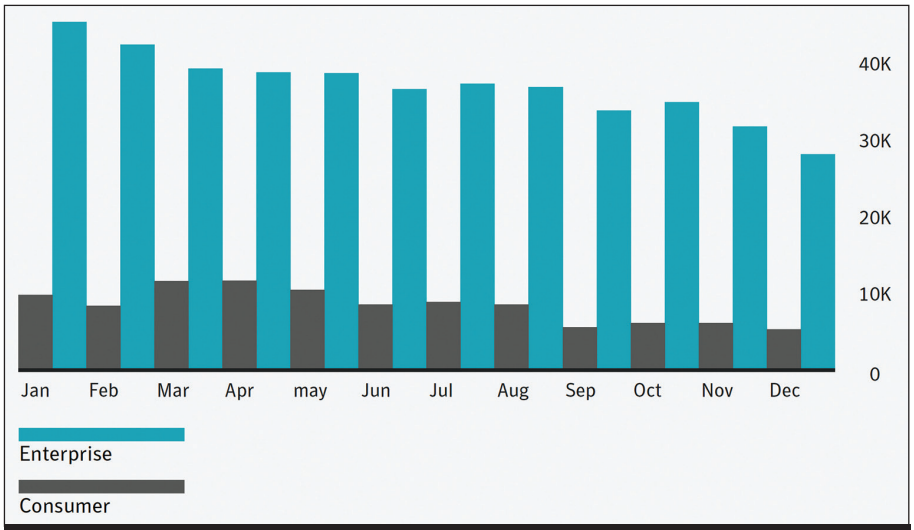
Identifying where these attacks could come from should form part of any risk management process and every organisation connected to the Internet must assume that it will be a victim sooner or later. Understanding this is the first step to assessing an organisation's vulnerabilities – but predicting how it could be compromised is not so easy.

Shifting landscape

The threat landscape is constantly shifting and businesses need to do all that they can to keep up to date. For instance, Symantec's latest report observes a decrease in ransomware activity for the first time since 2013.[3] This shift is probably due to a decline in exploit kit activity and a move to email campaigns as the chief ransom-

Of the top 10 short-term risks that respondents to a World Economic Forum survey expect to increase in 2019, cyber attacks appear at positions four and five. Other cyber-related risks in the top 10 include fake news and personal identity theft. Source: World Economic Forum.

ware distribution method. However, this exposes those organisations that are heavily dependent on email traffic – leading to enterprise infections increasing by 12%. Symantec also noted an increase in formjacking attacks, with an average of 4,800 websites compromised with formjacking



Ransomware attacks by market by month in 2018, showing a drop over the course of the year. Source: Symantec.

code each month. It's often small and medium-sized retailers that have code injected into their sites which can then spread globally to any business that accepts payments online.

Organisations also have to adapt their defence strategies as breaches can occur through the cloud, from vulnerabilities in hardware chips, through open source DevOps and by infecting Internet of Things (IoT) devices. And this adaptation is not an easy process for organisations to achieve, especially at a time when it is increasingly difficult to recruit and retain technically adept cyber security professionals.[4]

As a result, all organisations need to adopt a cyber security-aware culture that is supported at all levels, from board members to office juniors, and is embedded in all decision making. Having the right policies and procedures in place is critical and this should also include any employee-owned devices. Cyber security should certainly be part of any organisation's key values. Penetration testing is one way to make sure this happens.

White hat hacking

Hacking is often carried out for political purposes, criminal intent or sometimes just for notoriety or fun. However, all methods seek to exploit an organisation's vulnerabilities and are illegal. On the other hand, hacking for research – for example, the use of honeypots or white-hat hacking – is legal.

"Cyber security should certainly be part of any organisation's key values. Penetration testing is one way to make sure this happens."

Penetration testing is a form of ethical hacking but, for clarity, in order for hacking to be classified as ethical there needs to be an agreement between the

ethical hacker and the organisation – with written approval from the organisation. Otherwise, according to the letter of the law – the UK's Computer Misuse Act 1990, for example – it's just hacking. More than that, any chosen security company should have the right credentials and qualifications aligned with independent industry bodies such as CREST.

In essence, the ethical hacker's assessment of a system's security needs to answer key questions: what information can intruders see? What can they do with it and does this all go unnoticed? There are also practical considerations that need to be considered such as how often the tests should be performed and which testing strategy should be deployed. Should the test be carried out internally or externally, in a targeted way, or as a blind or double-blind test? Each organisation will have a preference but, essentially the penetration test will take on one of four forms – web application; infrastructure; mobile device and mobile application; and red teaming.

The average cost of a data breach, per record. Source: Ponemon Institute/IBM.

Web application penetration testing

This can be approached in several ways. It can be performed from the angle of an attacker who would initially know nothing about the configuration of the application (blackbox testing). Or a full review of the external aspects and internal configuration of the application can be carried out, including such elements as APIs, databases and user configuration (whitebox testing).

A typical test would consist of:

- Information gathering: Outdated framework versions, hidden content, user enumeration.
- Configuration: HTTP methods and headers, old back-up references, sensitive information within client-side code.
- Secure communications: Login encryption and cryptography methods in use (SSL versions and certificates).
- Session management: Cookie flags, scope and duration, session management.
- Authorisation: Path traversal, privilege escalation.
- Data validation: Testing for security vulnerabilities such as SQL injection (SQLi), cross site scripting (XSS) and XML external entity (XXE).

Infrastructure penetration testing

This method sees ethical hackers testing all elements of the infrastructure from servers and routers to switches, firewalls and endpoints, such as PCs and laptops. It should enable organisations to understand the security of their network from an internal and external perspective and involve multiple manual and automated enumeration techniques to systematically compromise systems in scope to establish the current threat landscape.

A typical infrastructure penetration test will consist of the following activities.

- **Planning and preparation**: Scoping.
- **Discovery**: Host discovery; port scanning
- **Enumeration**: Service enumeration and fingerprinting; vulnerability assessment.
- **Exploitation**: Compromise; privilege escalation.
- **Clean up**: Removal of any files/tools that the penetration tester may have used.
- **Report generation**.

Mobile devices and applications

Mobile device penetration testing can be the act of performing a security assessment against devices that access or hold sensitive information. It includes their physical security as well as performing penetration tests against applications that are created specifically for mobile devices such as applications on the iOS and Android platforms – this type of testing is similar to a web application test.

Red teaming

Whereas ethical hacking focuses on testing one specific element of an organisation's infrastructure and has a particular goal – for example, gaining access rights to a system – red teaming takes things further.

A red team engagement is a full-attack simulation that focuses on all areas of a business, from breaching networks and systems, to using social engineering tactics and gaining physical access to premises and devices. It helps identify critical issues that need remediation. The simulation also takes a lot longer than traditional penetration testing, with engagements lasting from a few weeks to a few months.

"The findings are presented back to the organisation with steps and suggestions to remediate the gaps and vulnerabilities. If, however, a critical issue is identified early on, this is flagged immediately to the business so that it can be fixed"

Typically, at the end of the exercise, the findings are presented back to the organisation with steps and suggestions to remediate the gaps and vulnerabilities. If, however, a critical issue is identified early on, this is flagged immediately to the business so that it can be fixed.

As an example, red teaming was used recently to assess a large financial services organisation. The approach was previously agreed with the client and it involved multiple attack vectors and a team with various skill sets. Key to the approach was a reconnaissance phase that allowed the team to build a detailed picture of the client, understand any potential weaknesses and then plan a credible attack strategy. These attacks consisted of gaining physical access to the building and connecting to the client network and, later, the client's main customer database. Social engineering tactics were used to create fake LinkedIn profiles, deploy malware onto the client's laptops and gain access to a large set of personal data files.

When presented back to the board there were no arguments – the company retained the team to help improve the organisation's internal security architecture to identify and prevent similar attack scenarios in the future.

Assurance, accountability and commitment

Ethical hacking is gaining traction within organisations across different industries as a significant way to improve their security posture and demonstrate accountability. Sometimes, it's even mandated by some risk and compliance frameworks, such as the Payment Card Industry Data Security Standard (PCI DSS) and the UK Government's IT Health Check that enables public sector organisations joining the Public Services Network (PSN).

Most recently, penetration testing has been highlighted as a key part of the General Data Protection Regulation (GDPR). Article 32 of the GDPR includes the requirement that there needs to be: "A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing".[5]

"In the event of a breach, organisations need to demonstrate accountability, that they have put the right practices and processes in place to mitigate risk. Penetration testing is one of the ways they can show this accountability"

In the instance of the GDPR, it's easy to see why penetration testing is held in high regard. All organisations know that the associated fines following a breach are significant – as much as €20m or 4% of global turnover. In the event of a breach, organisations need to demonstrate accountability, that they have put the right practices and processes in place to mitigate risk. Penetration testing is one of the ways they can show this accountability.

The value of ethical hacking

With the WEF confirming that cybercrime is one of the biggest threats to businesses, it does seem surprising that in a recent report, only 38% of business leaders said that improving cyber security was a priority for their IT investment.[6]

These threats are not going to go away, so the key question for many businesses is: do we really need penetration testing? In today's environment, the answer will always be yes. Of course, penetration testing is seen as a costly exercise. However, as with most things, organisations need to balance the cost with the risk of an attack. For some, the cost of an attack is more tangible – for example, is the business heavily reliant on an online application to process personal data that can be stolen? Or is its network and infrastructure critical to the business? This makes

penetration testing an easier sell to the C-level executives or financial director. For others who don't process sensitive data, the impact of an attack or breach could include reputational damage or irate customers as the result of downtime on a website.

Conclusion

The Ponemon Institute calculates the average total cost of a data breach to be $3.86m in its 2018 report.[7] This includes the costs associated with lost revenues, regulatory fines, damaged reputations and costs to recover from an attack. This translates to an average cost of $148 for every compromised employee or customer record (and more in certain countries, such as the US), so it is easy for organisations to work out the potential costs of compromise.

Data breaches may not account for all hacking attempts, but if the hackers are doing it for monetary reasons, then your data assets will be what they want. Organisations may not have an unlimited budget to spend on cyber security, but a penetration test can help to prioritise spending in key areas and prevent unnecessary spend in others.

"Attackers are becoming more sophisticated – so the longer an organisation waits to act, the greater the risks. Penetration testing should play a key role in identifying and mitigating these risks"

There are tools available for carrying out penetration testing in-house, but those that place their faith in a third party, one with the appropriate experience and accreditations, reap the most rewards. Penetration testing and red teaming combine to help organisations identify gaps and vulnerabilities in networks, devices and infrastructure, with the end result of mitigating an attack. In addition, these measures may be required for certain compliance frameworks and can be used to demonstrate a commitment, both to customers and employees, as well as securing more buy-in from the board.

The threats are not going to go away. Attackers are becoming more sophisticated – so the longer an organisation waits to act, the greater the risks. Penetration testing should play a key role in identifying and mitigating these risks, now and on a regular basis moving forward.

About the author

Scott Nicholson is technical delivery leader for Bridewell Consulting (www.bridewellconsulting.com). He has delivered security and privacy solutions on a global scale within a number of sectors such as central government, police, financial services, police, retail, oil and gas and has also worked with a number of software development companies, cloud service providers and some of the largest hosting companies in the world. Before joining Bridewell, Nicholson operated across a number of industries. His most recent roles before joining Bridewell were director of security and head of security and compliance. Working with companies ranging from SMEs to organisations such as IBM, he has provided a mixture of security leadership and technical delivery of programmes such as ISO27001:2013, PCI DSS, NIST, Cyber Essentials Scheme, PSN, PSNP and CESG (now NCSC) guidance.

References

1. 'The Global Risks Report 2019'. World Economic Forum. Accessed Apr 2019. www.weforum.org/reports/the-global-risks-report-2019.
2. 'UK small businesses targeted with 65,000 attempted cyber attacks per day'. Hiscox. Accessed Apr 2019. www.hiscoxgroup.com/news/press-releases/2018/18-10-18.
3. '2019 Internet Security Threat Report'. Symantec. Accessed Apr 2019. www.symantec.com/security-centre/threat-report.
4. Touhill, Gregory. 'Challenges on Cyber security Landscape Demand Strong Leadership'. ISACA, 20 Mar 2019. Accessed Apr 2019. www.isaca.org/Knowledge-Centre/Blog/Lists/Posts/Post.aspx?ID=1154.
5. 'Article 32, EU GDPR, Security of processing'. PrivazyPlan. Accessed Apr 2019. www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.htm.
6. Johansson, Grace. 'Cyber attacks one of the biggest threats to the world in 2018 says WEF'. SC Media, 18 Jan 2018. Accessed Apr 2019. www.scmagazineuk.com/cyber attacks-one-biggest-threats-world-2018-says-wef/article/1473450.
7. '2018 Cost of a Data Breach Study: Global Overview'. Ponemon Institute and IBM. Accessed Apr 2019. www.ibm.com/downloads/cas/861MNWN2

The Sandbox

Fighting fraud

Ryan Wilk, NuData Security

With security awareness on the rise, along with the introduction of new regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act, it's clear that the digital landscape is changing. The problem is that despite new rules, regulations and a higher level of awareness, fraudulent activity remains a growing challenge. The issue is so pervasive that out of 400 billion events monitored worldwide over the course of a year, 28% were high-risk fraudulent activity (http://bit.ly/2LwOJZh).

The same data showed that the volume of fraudulent activity is actually increasing by emulating the way that consumers interact with an organisation's pages. To put it simply, bad actors mask themselves alongside a company's good traffic, rendering it more difficult to identify a potential threat. Given these findings, it's more important than ever before that companies of all sizes and across all industries not only embrace better security awareness but also put it into action with improved policies and tools.

As companies scramble to get up to speed with bad actors' ever-evolving tactics, it's important to note that not all fraud is created equal. The distribution between mobile and desktop is vastly askew with mobile seeing 78% of traffic, while desktop had just 22%. This is important to mention because mobile malware is a major threat to businesses across various industries, especially those in e-commerce and banking. Kaspersky Lab indicated that the number of attacks using malicious mobile software nearly doubled in 2018 over the previous year (http://bit.ly/2PISxEV). Magecart, for example, has already wreaked havoc on several notable e-commerce companies, including British Airways, Newegg and Feedify, among others, and is still going strong in 2019 (http://bit.ly/2ISUpdX).

There's a lot of abuse in the merchant world, but one of the things that's high on that list involves trial fraud (think free trials or coupons for signing up or being a loyal member). Bad actors will use credentials to create new accounts and will sell these free trials for a minor payout. Over time, however, these 'free' sales can add up to hefty amounts.

New credit lines with instant approval are also a major target that quickly add up to unbearable losses. According to a recent report, in 2018 alone it took more than 53 million hours to clean up the mess of new account fraud.

This might seem like a no-brainer but having great tools is an absolute must. Even the most skilled security teams need equally smart equipment. The bottom line here is that every business needs functionality that allows its security protocols to evolve with the bad actors' techniques.

Behavioural biometrics plays a key role in this area by allowing organisations to better understand where threats are coming from. This reinforces real-time risk mitigation behind the scenes. By continually monitoring activity with these tools, security teams can actually see where threats are coming from and be prepared for an attack when it does happen.

Rules and policies are also vital. Security leaders need to ensure that all local laws and regulations are accounted for. Because there is no one-size-fits-all approach when it comes to running a secure business, it's essential that these policies are tailored to meet the organisation's specific needs.

EVENTS

3 June 2019
European Data Protection Summit
London, UK
https://summit.dataprotectionworldforum.com/

3–4 June 2019
International Conference on Cyber Security and Protection of Digital Services (Cyber Security)
Oxford, UK
www.c-mric.com/cs2019/

3–4 June 2019
Cyber Incident
Oxford, UK
www.c-mric.org/ci2019

4–6 June 2019
InfoSecurity Europe
London, UK
www.infosecurityeurope.com

10–12 June 2019
International Symposium on Digital Forensic and Security (ISDFS)
Barcelos, Portugal
http://isdfs.org

16–21 June 2019
FIRST Conference
Edinburgh, UK
www.first.org/conference/2019/

16–20 June 2019
Hack in Paris
Paris, France
www.hackinparis.com

17–20 June 2019
National Homeland Security Conference
Phoenix, AZ, US
www.nationalhomelandsecurity.org

18–20 June 2019
Infosec in the City
Singapore
www.infosec-city.com