STRATEGY / INSIGHT / TECHNOLOGY

info security

A New Dawn For Data Privacy Rights

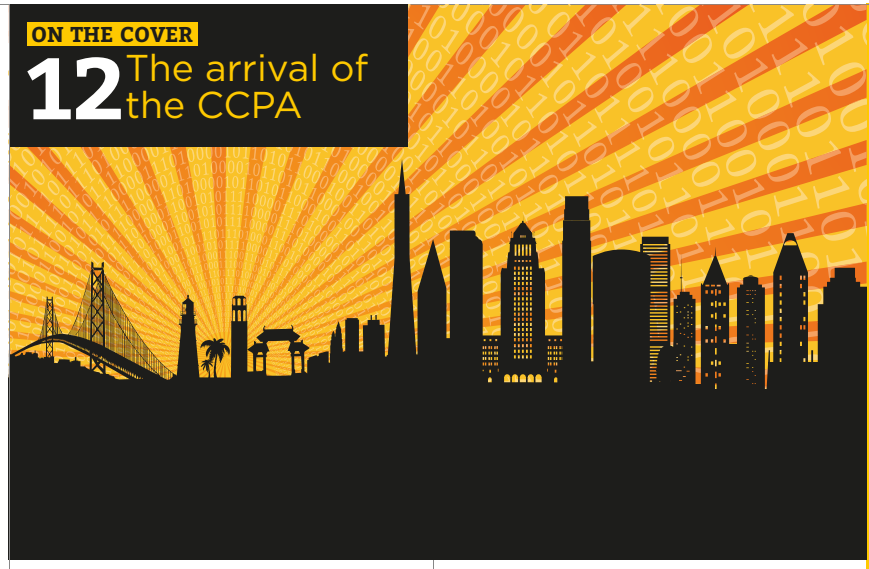
Q1, 2020 / Volume 17 / Issue 1

TO SELL OR NOT TO SELL?
Ethical considerations for vendors

RETHINKING RECRUITMENT
Solving the skills shortage puzzle

THE DIGITAL TRANSFORMATION JOURNEY
Why security is key

CONTENTS



The Contributors...

Eleanor Dallaway

Editorial Director
With more than a decade in the industry, Eleanor knows more about infosec than most English graduates should. Any small gaps in her social life are reserved for a good book and even better glass of wine.
@InfosecEditor

Michael Hill

Editor
With his degree in English Literature & Creative Writing and his love of the written word, Michael is dedicated to keeping *Infosecurity* readers up-to-date with all the latest from the infosec industry.
@MichaelInfosec

Dan Raywood

Deputy Editor
Dan has written about IT security since 2008. He has spoken at 44CON, SteelCon and Infosecurity Europe, as well as writing for a number of vendor blogs and speaking on webcasts.
@danraywood

James Ingram

Digital Sales Manager
James sells print advertising for *Infosecurity* and is also responsible for selling across all the online marketing and advertising options, including webinars and white papers.
@infosecJames

Infosecurity Magazine

Infosecurity Magazine

@Infosecurity Mag

info security

Editorial Director **Eleanor Dallaway**
eleanor.dallaway@reedexpo.co.uk
+44 (0)20 89107893

Editor **Michael Hill**
michael.hill@reedexpo.co.uk
+44 (0)20 84395643

Deputy Editor **Dan Raywood**
dan.raywood@reedexpo.co.uk
+44 (0)20 84395648

Online UK News Editor **Phil Muncaster**
phil@pmmediauk.com

Online US News Editor **Sarah Coble**
sarahcoblewrites@gmail.com

Print and Online Advertising
James Ingram
james.ingram@reedexpo.co.uk
+44 (0)20 89107029

Joel Marcus
joel.marcus@reedexpo.co.uk
+44 (0)20 89107028

Publishing Director
Rebecca Harper
Rebecca.harper@reedexpo.co.uk
+44 (0)20 89107861

Digital Marketing Manager
Karina Gomez
karina.gomez@reedexpo.co.uk
+44 (0)20 84395463

Senior Digital Marketing Executive
Ankita Bulsara
ankita.bulsara@reedexpo.co.uk
+44 (0)20 8910 7751

INFOSECURITY GROUP

Director **Saima Poorghobad**
saima.poorghobad@reedexpo.co.uk
+44 (0)20 84395683

Head of Sales **Abiola Agbalaya**
+44 (0)208 9107817

Production Manager **Andy Milsom**

ISSN 1754-4548

Locklizard

Share and Sell Documents Securely

Stop piracy of your training courses, ebooks, reports - protect and expand revenue streams.

Control document use inside and outside your organization - securely share with third parties.

Protect, control & analyze documents on any device

Benefits: Selling information

- Protect IPR from piracy
- Stop misuse of information
- Reduce publishing costs and time
- Prevent revenue loss
- Establish new revenue streams

Benefits: Internal use

- Protect IPR from disclosure
- Stop misuse of information
- Comply with regulatory requirements
- Enforce document retention policies
- Know when documents are viewed/printed

Stop Sharing | **Stop Printing** | **Expire Access** | **Track Use** | **Lock to Location**

Visit us at **www.locklizard.com** for your FREE 15 day Trial

Online Summit

INFOSECURITY MAGAZINE

INFOSECURITY MAGAZINE ONLINE SUMMIT

25th – 26th March 2020

14 Sessions | 12 CPE's | 2 Days | 1 Device | 0 Travel

- **Watch industry thought leader panel sessions covering key industry challenges, case studies & offering real world learnings**
- **Attend short form 30 minute "How to" sessions featuring technical specialists**
- **Download some of the lastest whitepapers, webinars, presentations, product information sheets and other data in our resource center**
- **Network & knowledge share in real time with industry peers globally through our new chat room**
- **Earn up to 14 CPE credits towards your SSCP®/CISSP®, ISACA & EC council certifications - fully integrated with your Infosecurity Magazine CPE management tool**

REGISTER YOUR PLACE TODAY

The full agenda and speaker line-up is available on our website.
We look forward to welcoming you!

WWW.INFOSECURITY-MAGAZINE.COM/ONLINE-SUMMITS/

@MichaelInfosec

From the Editor...

The Road Goes Ever On

It's a new year, a new decade, and the adage 'out with the old, in with the new' seems pretty apt for 2020

Firstly, it's a new dawn for the privacy rights of consumers – at least in the state of California. Yes, the California Consumer Privacy Act (CCPA) is now in force, coming into effect in January and bringing with it a host of new privacy rules and guidelines which companies must adhere to regarding the personal data of customers. It's widely regarded as the most ambitious piece of privacy legislation in US history, and it gives residents living in California various new rights including (but not limited to) the power to:

- Know what data is being collected about them by companies
- Know whether data is being sold to other parties, and to whom
- Refuse such sale of personal data
- Access their personal data

A particularly interesting element of the new Bill is the fact that, whilst it only protects and defends the data privacy rights of Californians, it will affect any companies that have customers based in California, regardless of where the companies themselves are located.

That means the CCPA has the potential to significantly impact not only enterprises across the US, but globally too. It is going to be fascinating to see what role the CCPA will play in the coming months and years, and how organizations cope with getting to grips with the new Bill. Our cover feature on page 12 chews the regulatory fat and outlines the major talking points, challenges and areas of importance of the CCPA.

This issue of *Infosecurity* also asks whether it's time to seriously rethink and reposition dated security recruitment strategies and replace them with new, fresh and forward-thinking approaches. The latest $(ISC)^2$ *Cybersecurity Workforce Study* estimates that the security skills gap has grown again, with global shortages now estimated to be more than four million professionals. Unsurprisingly, over half (51%) of the cybersecurity pros that $(ISC)^2$ surveyed in the study said their organization is at moderate or extreme risk due to staff shortages.

Clearly, traditional recruitment strategies within security have failed, so what needs to be done to bring about real, effective change in how the industry goes about recruiting talent in the numbers that it needs? Find out on page 22 as *Infosecurity* explores if, and how, the security skills shortage puzzle can be solved.

Furthermore, this year could be one in which our old foe ransomware starts to target a range of newer victims in bigger, more damaging ways. We saw the trend begin in 2019 – especially during the second half of the year – with the ransomware attacks that significantly impacted a number of municipal entities, from states and cities and towns, to local schools and councils. The attacks signified a notable shift from the traditional ransomware targets of enterprises and established businesses in the private sector, to entities in the public sector who arguably possess more sensitive data, but typically have far less sophisticated security means at their disposal. This issue's news feature on page 8 investigates just how that trend might manifest in 2020 and what it could mean for the security of data across the wider public sector.

It's a new dawn for privacy rights in the state of California

Another RSA Conference is just around the corner – the Infosecurity team will be at the event to bring you all the latest from the show

Finally, at a time when more and more organizations are embarking on complex journeys of digital transformation to modernize their businesses, our feature on page 28 highlights the key role that security must play in ensuring enterprises are digitally-transformed safely. Companies that fail to integrate security into every step of their digital transformation journey do so at their peril.

As you can see, there's plenty to cast your eyes over in this issue, and if that's not enough infosec action for you, we are also just a few weeks away from RSA Conference 2020 in San Francisco, February 24 – 28.

As ever, the *Infosecurity* team will be at the event, and we'll be bringing you a variety of content covering all the latest news, insight and analysis from the conference. If you are one of the tens of thousands heading there yourself, make sure you drop by booth 4139 and say hello to the team!

Finally, as we embark on a new chapter in cyber-history, I have no doubt that the next decade will bring with it various information security challenges and hurdles, and that the industry will be greatly tested as it continues its fight to keep people's data safe. However, I do believe that the world is a more cyber-secure place than it was 10 years ago, and the great many security strides made throughout the last decade prove what is possible with the right desire, investment and hard work. Long may that continue.

I hope you enjoy the issue, and I wish you the very best for the first quarter of 2020.

Michael Hill,
Editor

NEWS FEATURE

RANSOMWARE RENNAISSANCE: A MAJOR PUBLIC SECT

Ransomware is on the rise again, and 2019 saw a spike in attacks targeting public sector and municipal entities. *Phil Muncaster* finds out more

There has been something of a renaissance in ransomware attacks over the past year. Global detections soared by 74% from H1 2018 to H1 2019, according to Bitdefender. Yet, although the high-water mark for infections was undoubtedly 2017, thanks to WannaCry and NotPetya, attacks never really went away. Although some hackers started to dabble with cryptojacking as an alternative way to make money, the ransomware business model has proven remarkably resilient.

While stand-out attacks on the likes of NorskHydro and Demant have cost the firms over $120m in combined losses so far, it was arguably the US public sector that was hardest hit in 2019. The question is, can local municipalities recover, and what lies in store for 2020?

Cities Under Attack

There is no doubt that attacks are on the rise. Recorded Future's senior solutions architect, Allan Liska, was able to find evidence of 46 ransomware attacks on state and local governments in 2016, dropping to 38 the following year and bouncing back to 53 in 2018. However, in the first nine months of 2019 alone, 68 state, county and municipal entities had been impacted, according to Emisoft.

These included the cities of Baltimore, which refused to pay a ransom in a decision costing it over $18m (thus far). On the other hand, many local governments, including Florida's Riviera Beach ($600,000) and Lake City ($460,000) did decide to pay up. That's despite a resolution passed at the United States Conference of Mayors (USCM) in July not to cooperate with online extortionists.

Reports described the Baltimore attack as one of the most severe ever experienced in the US, "affecting nearly every important aspect of city life." However, even in less severe incidents, local civil servants have often been forced back to using pen and paper, as email systems are taken offline, billing and payroll systems suffer outages, the criminal justice system grinds to a halt, and in some cases even emergency services are impacted.

Attacks have also had an impact on local schools. In the first nine months of 2019 there were an estimated 62 incidents involving school districts and other educational institutions, potentially impacting operations at over 1050 schools, colleges and universities, according to Emisoft. In the case of the Moses Lake School District, which covers 16 schools, the district decided to back up data from three- to four-month-old copies rather than pay the $1m ransom. Crowder College reported a massive $1.6m demand, whilst Monroe College in New York was hit with a $2m ransom note in July.

For schools, as for local government offices, the rationale is the same: hackers know these organizations may be less well protected than many private sector firms, but run critical public services that may force them to pay up or risk chaos.

A Growing Attack Surface

"The greatest challenges they face are their use of legacy operating systems and the vast ecosystems of entities whom they support and therefore must implicitly trust," says Tom Kellermann, cybersecurity strategist at VMware Carbon Black and former presidential commission appointee. "This exacerbates their attack surface, making it easier than ever for sophisticated hackers to enter and steal valuable information and data."

Often, attacks have involved hackers using island hopping techniques to compromise municipalities via the MSPs and ISPs that provide them with services, he adds. For example, in August, 23 local government entities in Texas were affected after an attack on their MSP.

"This exploitation of the information supply chain has become commonplace," Kellermann tells *Infosecurity*.

Kevin Lancaster, general manager of security solutions at Kaseya, also believes increased media coverage may have piqued the interest of cyber-criminals.

"Even though data shows that governments often do not pay the ransom, there could be a false perception among malicious attackers that they do, due to the extensive media coverage of these kinds of attacks," he tells *Infosecurity*. "The resulting media coverage may also play into the ego of the attackers."

In fact, this certainly appears to be the case if we look at the ever-increasing ransom demands on local government and school organizations this year. It may also be the case that hackers are encouraged to launch copycat attacks if they read that a municipality has agreed to pay up because they were insured.

Time to Fight Back

On the plus side, most of the attacks we've seen over the past year in the US

OR THREAT FOR 2020

appear to have been using similar TTPs. These mainly revolve around social engineering in the form of malware-laden phishing emails, or targeting of Remote Desktop Protocol (RDP) clients, specifically through brute force/credential stuffing attacks.

According to Scott Styles, data orchestration and resiliency lead at Raytheon Intelligence, Information and Services, this means that a few common best practices – like AV, up-to-date patches, optimal configuration management, and back-ups – can have a big impact.

"In addition, a 'defense in-depth' approach should be a top consideration to stay ahead of future threats. Ransomware, by its very nature, uses the operating system and its resources to carry out an attack. Therefore, hardening the operating system and underlying hardware can address a wide variety of advanced persistent threats and zero-day exploits posed by malware," he tells *Infosecurity*.

"Lastly, organizations should consider implementing a 'data-driven' approach that can differentiate between normal processing and ransomware behavior. This approach leverages the operating system and underlying hardware to enhance the behavioral analysis and machine learning necessary to automate and accelerate the response to a ransomware attack in near real-time."

> ***"The greatest challenges [public sectors] face are their use of legacy operating systems and the vast ecosystems of entities whom they support and therefore must implicitly trust"***

This approach should be used alongside a strong backup and disaster recovery plan, according to Kaseya's Lancaster.

"A foolproof method of backing up data would be a combination of onsite and cloud backup, also known as hybrid cloud backup. An onsite backup is especially handy when facing internet connection issues due to system disruption, and is highly efficient and less expensive than other methods," he explains. "Remember, backups are only as good as your recovery. Periodically test the restore process to ensure that restored files from backups are accurate. If the worst happens, you should be able to recover your data without thinking and get it back exactly the way it was before."

The Bigger Picture

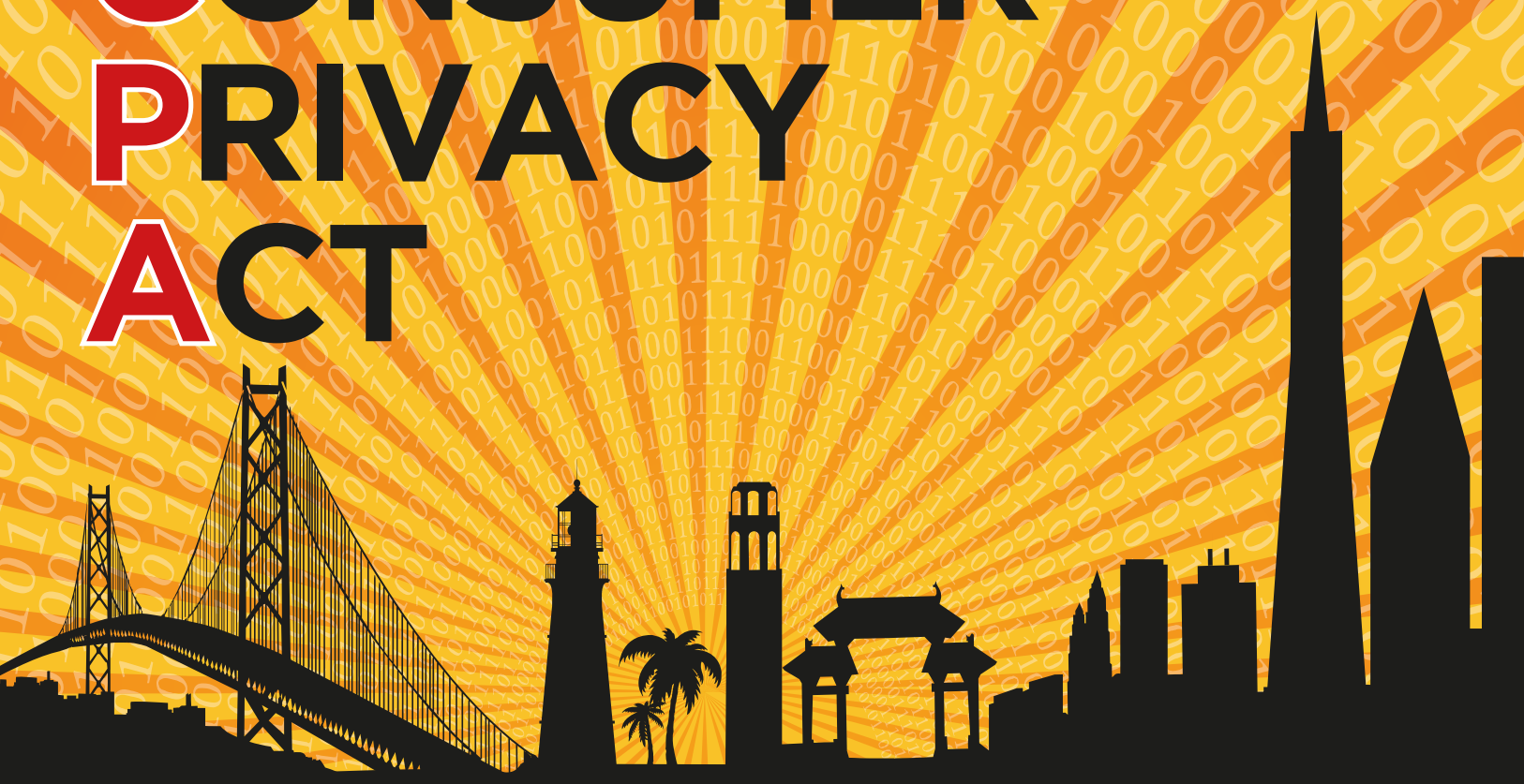
This is all very well, but funding shortfalls can make these investments problematic, according to Johannes Ullrich, SANS Institute dean of research.

"Public entities often have a hard time articulating the need for a sufficient investment in information security and disaster recovery. Spending often lacks coordination across IT departments which are organized by political structures versus functional and business structures," he says. "Public entities also have a hard time competing for talent, not just due to problems matching private sector compensation, but also due to work environments that do not attract the type of individuals required to perform cutting edge information security work."

Yet progress is possible. Louisiana state governor John Bel Edwards set up a Cyber Security Commission to help local municipalities respond quicker to emerging threats, which they needed to do twice in 2019 after ransomware attacks struck. The senate has also passed a new law which will require the Department of Homeland Security (DHS) to build dedicated teams tasked with providing technical support and incident response assistance to affected organizations.

With fears that ransomware could be used to disrupt the 2020 Presidential elections, recognition of the threat at a federal level has come not a moment too soon. As bad as the impact of attacks has been on local municipalities over the past year, serious interference in November could only serve to magnify the issue END

CALIFORNIA CONSUMER PRIVACY ACT



Danny Bradbury shines a light on the arrival of the CCPA and examines what it means for the future of data protection in California

A NEW DA PRIVACY

AWN FOR
Y RIGHTS

It's here, it's in force, and if you're doing business in California, it should be on your radar. It's the California Consumer Privacy Act (CCPA), and it's the most ambitious piece of privacy legislation in US history. It marks a new dawn for the privacy rights of consumers in California. If you haven't already prepared for it, then you're extremely late, and your business is potentially vulnerable.

Passed on June 2018 within a week of its introduction, it is also among the fastest. It came into effect on January 1, and if your company does business with anyone in California, then it affects you. If you have not taken steps to comply with it, there is no time to lose.

The law introduced a swathe of new measures that hold companies accountable for their use of citizens' personal data and put them on a similar track to those dealing with Europeans under the General Data Protection Regulation (GDPR). Companies are subject to the legislation if they collect a consumer's personally identifiable information (PII), if they do business in California, and if they fit one of the following conditions: make more than $25m per year, commercially process PII from at least 50,000 consumers, households or devices, or derive more than 50% of their revenue from selling consumers' personal information.

The penalties for data breaches under the Act are daunting. A company could pay up to $750 per incident to each consumer ($750,000 for the theft of a 1000-consumer database), or actual damages, whichever is the greater. The State can also fine them up to $7500 per consumer for each intentional violation. Given the size of some breaches these days, that represents a massive potential penalty.

> ***"Most businesses in the US that are cross-state will be affected by this"***

One of the biggest misconceptions among US companies outside California is similar to one that also led US businesses astray in the run up to GDPR, warns Corey Nachreiner, CTO of application firewall company WatchGuard: companies are wrong to think that they are not affected if they are based outside California.

"Most businesses in the US that are cross-state will be affected by this," he warns. That includes businesses selling online.

The Effects on Business

Those companies that have already grappled with GDPR will find the California requirements "more of an evolution," explains Caitlin Fennessy, research director at the International Association of Privacy Professionals (IAPP).

Those companies that are operating only in the US and haven't yet built out a strong privacy program are the ones that will have a lot of work ahead of them, she adds.

Part of that is down to what Fennessy describes as a broad definition of personal data under the CCPA when it comes to the legislation's data breach provisions. It includes anything that could be directly or indirectly linked to a consumer or household. That could include an alias or other online identifier, cookies, a device identifier, pixel tags, customer number and even information linked to a household. It also includes things not generally listed under US data privacy legislation, like purchasing histories, internet activity including browsing patterns and inferences drawn about consumers using their data. As such, it goes even further than the GDPR in its definition of personal data.

The law offers consumers several private rights of action, including the right to find out what information a company holds about them and into which categories it falls, which categories they sold and to whom, and where that data came from. Businesses must provide that information in a portable format, and they must honor requests to delete it.

Fennessy also points to the need to provide a button on a home page and on all pages collecting information that enables the visitor to opt out of having their information sold to third parties. The definition of 'selling' is also pretty broad, she explains.

"It depends on whether the entity with which you're sharing data is processing the personal data for the original entity's business purpose on behalf, and under the instructions, of the original business, and that relationship has to be governed by a contract," she explains. That will affect a wide variety of companies, including those in the adtech space, she says.

Enforcement Issues

Timelines aside, Fennessy also points to the intent of the California State Government and private individuals. "The California Attorney General (AG) has been very clear that they do not intend to take a 'gotcha' approach here," she says. "They want companies to work diligently to come into compliance, but they're not looking to catch folks out."

Outside the data breach provisions, there is also a 30-day 'period to cure' timeline to fix privacy violations, says Mariani, so that companies can address their problems before penalties come into play.

However, that doesn't mean that the AG won't bring measures to

firm up the interpretation of the law, Mariani argues. Big tech could fight a government case on the grounds that the law was ambiguous, so building a series of established settlements with other companies (known as assurances of discontinuance) would help to prevent that strategy. That means hitting smaller companies with fewer resources.

"I would go after the companies that I think I could get settlements for," he suggests. "That would help me push out what the law means to other businesses so I can enforce the law more."

The AG isn't the only litigant that companies playing fast and loose with customer data should worry about, Mariani adds. They could risk severe penalties for both data breaches and other privacy infractions under the private right of action provisions, he warns.

What to Do About It

That means companies that have left things late and are struggling to catch up should focus on several core things. If they haven't thought about data governance until now, then they should look at what they're collecting, why, and what they're doing with it, advises Mariani.

For many companies, that will involve a data audit using some kind of automated tool, says Nachreiner.

"So make sure you look for tools that can help do that data audit, and can classify not only the personal data, but a lot of metadata, that's going to be considered PII as well."

As the sale of data stipulations in the legislation use contractual relationships to determine whether a company is liable under CCPA, it's also important to assess those contracts, warn experts. If you are transferring data to others, then you must push obligations to treat that data lawfully downstream to those partners, he warns.

The AG's proposed guidelines for complying with CCPA also mandate training for any employees tasked with handling consumer inquiries about the company's privacy practices.

> ***"They want companies to work diligently to come into compliance, but they're not looking to catch folks out"***

Under CCPA, the private right to action measures came into effect first on January 1 2020. The State's ability to enforce CCPA won't kick in until July 1 2020, or whenever proposed regulations fleshing out the law are approved, whichever is sooner. Companies should focus first on creating systems to service those private right of action needs, says Mariani.

Ideally, this will be an automated system to provide transparency about how data is used, but companies who are already in violation may have to fall back on manual procedures for now. The draft regulations enforcing the law also dictate the use of verification systems to authenticate the identity of people asking about their data, warns Fennessy; you don't want to inadvertently give a customer's data to an imposter and break the law.

Other measures to begin with include updating privacy notices and also implementing an information security program. Absent of any firm guidance, companies can look to the Center for Internet Security's Cybersecurity Controls. Former AG Kamala Harris said that failing to implement these indicated a "lack of reasonable security" in a 2016 report on data breaches.

What Happens Next?

Companies cannot afford to do nothing in their CCPA compliance, warn experts; but it won't be the only strict privacy law to pass.

"Bills are percolating in other states like WA, NY and IL," explains Michelle Richardson, director of the Center for Democracy and Technology's privacy and data project. However, these may take some time to bear fruit.

"We are watching closely but it's hard to predict which ones can build the coalition necessary to pass such a sweeping proposal," she continues. "Most states have much shorter sessions than California – this is even harder when legislators have to work in annual two or three month bursts."

There's also the fact that many states don't have ballot initiatives, points out Mariani. Alistair McTaggart, the real estate mogul who conceived the CCPA, could only do so because he was able to force big tech's hand by beginning the effort as a ballot.

While states continue to push the issue, there are also movements at the federal level. Until now, federal privacy law has been a patchwork of sector-specific measures like HIPAA and enforcements by the FTC, often under the FTC Act. Dedicated privacy laws are only just now hitting the hustings. One of these is Senator Ron Wyden's Mind Your Own Business Act (formerly the Consumer Data Protection Act) which would introduce fines and potential time for CEOs or chief privacy officers that flouted the rules.

For businesses that have not yet come to grips with the CCPA, there's no time to lose. The law already allows private individuals to launch actions against businesses that violate these strict privacy rules and the State's ability to penalize them will kick in soon. It is time to talk to your lawyer, and your tech team, today END

info security
STRATEGY | INSIGHT | TECHNOLOGY

ATTEND OUR EXCLUSIVE INFOSECURITY MAGAZINE EVENTS!

The *Infosecurity* Magazine team hosts a series of luxury briefing events and roundtables alongside globally-renowned industry conferences and exhibitions around the world.

Join us at one of our upcoming events to:

- Participate in topic-focused conversations, led by thought leaders and experts
- Network with an exclusive group of CISOs, team leaders and exclusive editorial guests
- Meet the *Infosecurity* Magazine editorial team
- Earn 1 CPE credit
- Enjoy a luxury breakfast, on us!

CONFIRMED DATES FOR 2020 INCLUDE:

BREAKFAST BRIEFING AT RSA
February 26, San Francisco, USA

BREAKFAST BRIEFING AT INFOSECURITY EUROPE
June 2-3, London, UK

WOMEN IN CYBERSECURITY SUMMIT AT INFOSECURITY EUROPE
June 3, London, UK

Stay in the know by updating your *Infosecurity* Magazine email preferences to receive 'Conferences' alerts.

WE LOOK FORWARD TO WELCOMING YOU AT ONE OF OUR EXCLUSIVE EVENTS!

https://www.infosecurity-magazine.com/magazine-events/

Q&A

TIM MACKEY

Tim Mackey is a security strategist who applies his skills in distributed systems engineering, mission critical engineering, performance monitoring and large-scale data center operations to solve customer problems. He takes the lessons learned from those activities and delivers talks globally at well-known events. When not working, Tim loves spending time with his Fortnite-, football- and BattleBot-mad son. Plus, a little chess challenge here and there doesnt hurt either!

By Michael Hill

How did you get into the information security industry?

It was an accident really. I spent my early career working on mission critical engineering projects. That taught me to think about the edge cases which enabled me to make the leap from saying "'it's a bug" to "it's a security issue." This mindset served me well when I joined the cross-functional product security virtual team at Citrix following an acquisition. The rest, as they say, is history. I moved into the world of virtualization, cloud and containers where the scale of security issues are always increasing.

What's the best thing about your job, and what's the worst thing?

By far the best thing about this job is being able to meet fellow security practitioners at global events. We all have our areas of focus, and perspectives, but being able to share those perspectives can be the proverbial 'lightbulb' moment for someone who is solving a problem. The worst part is dealing with an incident. Thankfully, I've been lucky and not had to deal with many, but they are challenging. To put it into perspective, as members of the public, pretty much everyone has received some notification of a data breach. What most people don't realize is the amount of work that goes on behind such a report, and how many comparably minor versions of such incidents occur each year.

What's your proudest career achievement?

I love mentoring and creating teams, and have had the good fortune to do both multiple times over the years. Often the best thing I can do is identify the right people, unleash them on a problem and watch the magic happen. This is why I value collaboration so much – innovation isn't a straight line, it's a series of zigs, zags and failures, with lessons learned along the way. Successful teams and outcomes are often more a function of sharing ideas than using brute force.

What would you do if you did not work in information security?

Those who know me best would likely say I would either be a 'mad scientist' or a travel blogger. I'm a fairly creative guy and quite willing to roll my sleeves up to figure out how things work. If in that effort I solve an interesting problem, there's a reasonable chance I'll try and make that solution into 'something.' As for becoming a travel blogger, I've had the good fortune of seeing far more of the world than most will and sharing my experiences probably taps into the same collaborative mindset I use elsewhere.

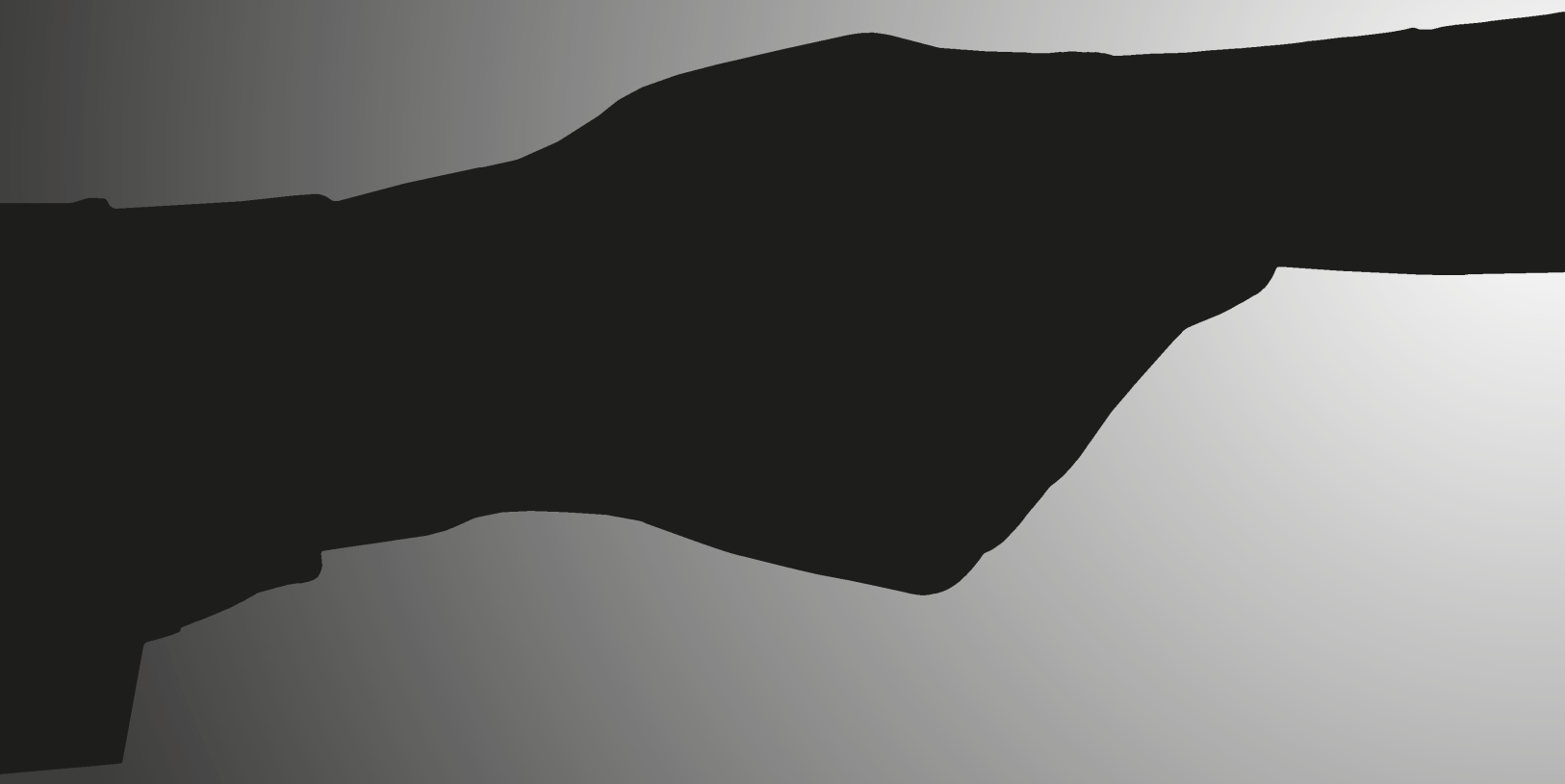
BIO

@TimInTech

Tim Mackey is senior principal consultant at the Synopsys Cybersecurity Research Centre. He joined Synopsys as part of the Black Duck Software acquisition, working to bring integrated security scanning technology to the Red Hat OpenShift and the Kubernetes container orchestration platforms.

TO SELL OR NOT TO SELL?

Cybersecurity is big business, but in the wrong hands, some tools can undermine national security and human rights. *Phil Muncaster investigates*



WHERE SHOULD VENDORS DRAW THE LINE?

In October last year, Facebook announced a bold move. It launched legal proceedings against a notorious Israeli 'cyber-intelligence' vendor, alleging it had helped to develop and then deploy malware later used to spy on innocent civilians in the Middle East and elsewhere. The case is an extreme example of what happens when ostensibly legitimate security tools are used and then abused. For countless western cybersecurity vendors, this is a growing area of business risk. So in our globalized economy, how best can these firms balance their commercial interests with ethical and legal considerations?

Even when the will is there to do the right thing, it can be a complex undertaking. However, the growing reputational and financial risks of not doing due diligence on exports makes this particular compliance task non-negotiable.

When Good Security Turns Bad

Cybersecurity is big business. The market for related hardware, software and services was forecast to top $106bn by the end of 2019, an 11% jump from 2018, and reach $151bn by 2023, according to IDC. As digital transformation sweeps the globe and cyber-threats escalate, Western security vendors quite rightly want to take advantage of soaring demand to protect IT systems in order to grow their profits. In fact, their governments encourage them to do so in order to drive economic growth for their respective countries.

Yet there is growing anxiety over the use of legitimate security products by authoritarian regimes and organizations operating in these countries. Surveillance technology is where most attention has focused up until now, but a range of cybersecurity tech can, in fact, be used with malign intent.

Deep Packet Inspection (DPI), for example, legitimately works to identify if content contains malware or not. It is used in intrusion prevention/detection (IPS/IDS) tools for this reason, and by network managers to prioritize mission-critical traffic. It can even help ISPs block DDoS attacks. However, on the other side, the technology can also be used to monitor legitimate internet traffic which poses no cybersecurity threat, but helps authoritarian regimes eavesdrop on journalists, rights activists, opposition politicians and others.

UK trade association techUK lists this, and many other security-related technologies that could also be abused, in its detailed 2019 document *Examining Cyber Security Export Risks*. Big Data analytics, social media analysis tools and forensics solutions could also be used to harvest data on specifically targeted individuals. Even identity and authentication platforms could be abused to monitor targets' movements, it warns.

Yet another example is content and URL/IP address filtering tools, used to support safer browsing among users. These could also be abused to restrict the free flow of information online. Canadian company Netsweeper has been called out in the past after its technology was used in just such a context, by ISPs in Afghanistan, Bahrain, India, Kuwait, Pakistan, Qatar, Somalia, Sudan, UAE and Yemen.

> ***"The hardest challenges to navigate are questions around 'dual-use' technologies, which can be sold for one purpose but then used for another, more nefarious task"***

Pushing the Boundaries

While many cybersecurity vendors will be aiming to keep their tools out of the hands of such regimes, there are some that seem to actively court notoriety by selling products and services which could be easily abused.

These include the UK/German company Gamma International and the aforementioned NSO Group. The former developed infamous spyware known as FinFisher, which the OECD alleged it sold to the Bahrain government, where it was used to monitor human rights activists there. NSO Group develops exploits and spyware, dubbed Pegasus, which it has been claimed was used in a similar manner to target over 100 individuals around the world.

Both firms, and many others, argue that they provide such capabilities to legitimate law enforcers and intelligence agencies and that they don't sell to repressive regimes. However, the stats tell a slightly different story. According to written evidence to parliament by Privacy International, of the 275 license applications for surveillance tech approved by the UK government between 2015-18, only a fifth (21%) of the destination countries were considered 'free' by Freedom House.

The rights group's state surveillance program lead, Edin Omanovic, believes that gaps in the UK's export regulations give too many vendors the opportunity to cross an ethical line.

"While the current controls designed to mitigate human rights risks associated with surveillance tech are weak and ineffective, no such controls exist for cybersecurity exports. This is a clear limitation of the current regulations which leaves people across the world vulnerable to surveillance and censorship," he tells *Infosecurity*. "While companies have due diligence obligations which indeed many take seriously, the idea that non-binding and unenforced risk assessments will stop every company from profiting from authoritarians around the world is clearly naive."

Do Governments Care?

In fact, the whole idea that government 'export controls' are there to restrict exports is a false assumption, according to Luta Security CEO, Katie Moussouris, who is helping the US government negotiate the global control regime known as the Wassenaar Arrangement. She argues that companies like NSO Group, Hacking Team and Gamma International were all given licenses by their respective governments.

"The reason is that export controls are not really there to restrict the export of items. They're there so governments can keep track of who

> *"Ultimately, organizations themselves have to make measured, reasonable decisions about the people they deal with and the territories they play in"*

is making what and whom they are selling it to," she tells *Infosecurity*. "They're still trying to work out how to conduct cyber-warfare fairly, and part of this is inspecting the weapons being used in this emerging class of warfare. The law of the sea took 100 years to develop, and we're only at the very beginning of this."

If this is true, then it places an even greater responsibility on the security vendors themselves to ensure that any decisions about who to sell to don't backfire.

Dan Patefield, program manager at techUK, argues that complexity is a key challenge, and that smaller vendors especially need more help to navigate the landscape.

"There is a wide array of cyber-capabilities, ranging from cutting-edge defense capabilities to basic cyber-hygiene for citizens. The hardest challenges to navigate are questions around 'dual-use' technologies, which can be sold for one purpose but then used for another, more nefarious task," he tells *Infosecurity*. "TechUK believes that the current frameworks for export controls relating to cybersecurity represent a sensible but complex approach which can be lengthy and difficult for companies, particularly SMEs, to navigate."

Adding to the complexity is the potential risk to corporate security, according to Amanda Finch, CEO of the Chartered Institute of Information Security (CIISec).

"If a vendor – especially a small vendor that relies on its IP to differentiate itself – has an opportunity to sell to a country or company that is notorious for stealing IP, they are likely to think twice," she says. "Also, there is potential access to source code. When selling its products, a vendor needs to consider all of its customers. A vendor with multiple government contracts working with a potentially opposed nation could be opening up its customers' most sensitive networks to their competitors."

The Importance of Due Diligence

The bottom line is that cybersecurity vendors must manage the risks associated with exporting their products, just as they do other business risks. This means choosing customers carefully: even if a license application is approved by the government, there could still be consequences in lost IP, customer attrition and reputational damage, if they make the wrong decisions.

"Ultimately, organizations themselves have to make measured, reasonable decisions about the people they deal with and the territories they play in, with the potential result of inaction being a harm to the reputation both of the company and the [country]," says Patefield. "TechUK and the government can only ensure that the right information is out there, in an easily accessible form, but we encourage companies to conduct a comprehensive due diligence process."

This is important at every stage, from product development, to pre-sales, point-of-sale and post-sales stages, according to the tech body. Vendors should first assess whether there are any relevant trade sanctions or embargoes, or export controls on the destination country, then conduct a full risk assessment if appropriate. In the UK, they should check with the Export Control Joint Unit (ECJU) if in doubt. In the US, it's the Commerce Department's Bureau of Industry and Security, although the State Department also has some resources on this.

Ultimately, every vendor must know its limits, understand where the ethical and business barriers lie, and ensure it doesn't break them, concludes CIISec's Finch.

"There are a number of complex commercial, legal, financial, technical and organizational decisions and trade-offs for vendors to make. Regardless of the final decision, they need to make sure they are acting consistently, in full understanding of the risks, and in line with their own values," she says. "If they have done this, then they will know whether to turn down an opportunity, or to pursue it knowing they are prepared for any potential consequences." END

What's the Wassenaar Arrangement?

The Wassenaar Arrangement is an international export control regime for conventional arms and dual use goods and technologies. Countries including the US and UK are members, and implement the decisions taken at this level into their respective export rules. However, controversy surrounding the voluntary arrangement highlights the challenges of multi-lateral decision making.

Luta Security's Katie Moussouris fought successfully for changes to the language which would otherwise have impacted legitimate vulnerability research and incident response activity.

A similar fight is now on to exempt pen testing tools and training from these export controls, she tells *Infosecurity*. If it fails, it could have a chilling effect on efforts to grow the cybersecurity workforce, she argues.

RETHINKING RECRUITMENT: SOLVING THE SKILLS SHORTAGE PUZZLE

As cybersecurity skills shortages continue to grow, *Davey Winder* explores why changes in recruitment tact are urgently required

Given the seemingly never-ending reports of data breaches across the last two years, coupled with mobile malware rising and ransomware finding new targets in healthcare and municipalities, it should come as no surprise that the cybersecurity industry is a hot potato right now. According to the 2019 (ISC)² *Cybersecurity Workforce Study*, there are some 2.8 million people working worldwide in the cybersecurity sector, with the US (804,700) and the UK (289,000) being the biggest cyber-employers. That's the good news.

The bad news is that it's simply nowhere near enough. Despite media headlines highlighting the cyber-skills shortage for a very long time, there's little sign that this workforce gap is shrinking; in fact, the opposite is happening. According to that (ISC)² report, the gap has grown since 2018 due to a global hiring demand surge. In the US alone, it is estimated to be around 500,000, and in Europe, 291,000. Globally, the cybersecurity workforce shortage is estimated to be some four million vacancies. That means the number of people working in cyber needs to grow by 145% just to catch up and stop the stagnation. To put that into some perspective, 65% of organizations represented in the (ISC)² survey had a shortage of cybersecurity staff and 51% of cybersecurity professionals said that this shortage was putting their business at risk.

So, what is wrong with security industry recruitment and how can the errors of the past be corrected to ensure the right talent, in the right numbers, can be hired moving forward?

Recruitment Isn't Working

"There are clear signs that IT security recruitment isn't working as needed," Amanda Finch, CEO of the Chartered Institute of Information Security (CIISec) says. "According to the Enterprise Strategy Group, the number of organizations reporting a problematic shortage of cybersecurity skills has increased every year since 2015." Does this mean that the cybersecurity industry needs to rethink its approach to recruitment? Finch is convinced that, unless things change, we will be facing a "stagnating" workforce that is unable to keep up with the expanding skills gap. "A large part of this problem is a result of where recruitment focuses its efforts," Finch explains. "Too often there is the expectation that security is a technical subject: meaning only people with an aptitude for tech, or the right technical qualifications, should be considered." This, in turn, results in recruitment from a narrow demographic. CIISec's annual survey this year revealed that 89% of respondents were male, and 89% were over 35. "Unless the industry rethinks its approach to recruitment by embracing greater diversity, in gender, age, ethnicity, disabilities and experience, businesses will continue to face reduced protection and over-worked security staff," Finch warns.

Placing too much emphasis on education, be that in terms of a university degree or industry certifications, is certainly the primary reason for recruitment failing the sector so badly, according to BeyondTrust CISO, Morey Haber. "Information security is much more akin to a vocational job that requires self-learning or training, but not a formal education," he insists. "To that end, the industry should look for passionate individuals that have an interest in cybersecurity and possess exceptional detective and deductive skills."

Anthony Young, director at Bridewell Consulting, agrees that many employers are far too shortsighted when it comes to recruiting cybersecurity professionals. "They expect to hire employees that have the knowledge and skills to cover the latest technology, solutions and threats," Young points out, "but it's impossible for an individual to be an expert in all areas concerning cybersecurity as the landscape is constantly changing." Which, Young adds, means that searching for someone that ticks all the boxes often means that truly talented individuals get overlooked. "Organizations should focus on identifying talented individuals who

have a real passion for cybersecurity and invest in training them up," he argues.

Filling the Gaps

As the talent pipeline is increasingly squeezed, the cost of recruiting the right talent increases, Graham Hunter, vice-president of skills at CompTIA says. "A more sustainable and strategically sound approach is developing talent in-house rather than fighting for resources in urgency," Hunter explains. "Lifelong learning needs to be adopted as habit, enabling employees to move up in the business and open up spaces for lower-level roles."

Is widening the talent pool criteria really all that needs to be done to break the skills gap impasse? If only it were that easy. "Many businesses are under-benchmarking and inaccurately scoping roles," says Ross Tanner, head of practice (information security) at La Fosse Associates. This means that cyber-salaries and years of tenure are often aligned to technology counterparts, or multiple remits are crammed into individual roles. "Unsurprisingly, it's common to find companies unsatisfied with their cyber-teams' outputs further down the line," Tanner says. Then there's the problem of putting way too much responsibility at the door of security

tools which are often considered to be some kind of silver bullet. "The common theme throughout security vendors today is 'automation' or 'artificial intelligence' in their products," he continues. "Without the right people in place to make sense of the outputs from those tools, companies are left with an ineffective and costly overhead that could be better spent on highly-skilled security specialists, or training to upskill existing staff."

There are forward-thinking recruiters out there, applying the kind of approaches needed to start shrinking the cybersecurity skills gap. So, what are they doing right that others have done so wrong? Diversity is the key factor according to Lynn Studd, director, BT Security, who says that recruiters need to look at attracting as diverse a range of potential employees as possible, "in particular, by thinking about what the barriers and the enablers of their careers are."

So, for example, BT "recognizes the skills that neurologically diverse candidates can bring to security, in particular around complex problem solving and pattern analysis," Studd says.

Amanda Finch certainly agrees that forward-looking organizations are expanding their reach when looking to attract the right people. "They look outside technology to find individuals with the right transferrable skills which can benefit a security role," she says. "For instance, tracking and managing multiple actions at once could easily be transferable from a parent returning to work, and teachers should be highly capable of demonstrating and explaining best practice." Finch is also seeing evidence of recruiters taking a framework-based approach rather than simply looking at CV keywords, which means identifying the capabilities a specific role needs, then matching those to candidates. "The framework-based approach to best practices and skills is a way of validating security skills and roles," Finch says, "ensuring that each role is really understood and clearly displays to new recruits the paths they can follow in the organization."

> ***"A large part of this problem is a result of where recruitment focuses its efforts"***

Give Everyone a Fair Shot

If there is one essential takeaway from the conversations *Infosecurity* has had with CISOs and cyber-recruitment specialists, it is this: everyone must be given a fair shot at an infosec career if any real progress is to be made in filling the skills gap anytime soon.

This simple-sounding notion is key, according to Joan Pepin, chief security officer at Auth0. "In general, there is a 'type' that has traditionally been the infosec practitioner," she says. "While you can find many examples of people who don't fit that, that idea has been propagated and, in some cases, defended and enforced." However, infosecurity recruiters need to be very careful when talking about any cultural fit. "It doesn't mean we play the same video games, watch the same shows, laugh at the same jokes, or go to the same movies," Pepin concludes. "It means we care about our jobs, our customers, and we're innovative and creative." END

Identifying In-Demand Skills for Modern Cybersecurity Roles

Firstly, we need to understand where the skill shortages sit within most organizations as far as cyber is concerned. "Currently we're not seeing a skills shortage at CISO level," Bridewell Consulting's Anthony Young says. "The real skills gap exists beneath CISO level, particularly around specialized technical skills like penetration testing or cloud security." So, while many companies are embracing AWS, Azure and Google Cloud, all too often they might not have all the expertise required to ensure that they are configured securely, as various reports of leaking data buckets confirm. This reveals an interesting reality: while in-demand skills vary widely across organizations based on size and specialization, they do follow technology trends. No surprise then that Morey Haber, CISO at BeyondTrust, sees "skills for the cloud, identity and privileged access, vulnerability, patch, and configuration management, and mobile device security," being firmly in demand. CompTIA's Graham Hunter agrees, insisting that "in-demand skills fall into the three main categories of modern security: technology, education and process." The most sought-after skills, though, remain firmly in the traditional category of technology. "Whether it is new practices that reflect a more proactive mentality (such as cybersecurity analytics), new tools that address cloud/mobile infrastructure (such as identity and access management), or new threats that take advantage of digital reliance (such as social engineering), Hunter says that "companies need their IT and security specialists to be up-to-speed on the changing technological landscape."

The changing landscape comes to the fore as far as Steven Cockcroft, director at Cybersecurity Professionals, is concerned too. "Some of the most in-demand skills that are lacking include compliance, risk management, framework implementation and auditing," he says. "These skills will become more essential in the years to come as more businesses adopt stricter cyber processes and need to consider the wider implications of their security strategies." Perhaps, then, the most in-demand skills will be transferable ones, and these are underutilized currently. "Framework implementation and auditing are strategy-based skills," Cockcroft concludes, "which will benefit from candidates who think in different ways."

Director's Cut...

Eleanor Dallaway, Editorial Director

As I was pondering what to write about in this issue's Director's Cut, I jumped onto Twitter in search of inspiration. The first tweet I saw was from @BrianHonan (Hey, Brian!): "Guess I need to stop working in #infosec. Not only do I not have a degree in computing, I also do not have any CVEs." Bingo, that's the inspiration I needed.

As an industry, we've bemoaned the so-called skills gap for as long as I can remember. I've lost count of the number of times infosec professionals have told me that finding, hiring and retaining talent are amongst their biggest challenges.

We often blame the people outside of our industry for this. We question why they don't want to work in cybersecurity. We talk about how they perceive the industry to be 'too geeky,' 'too techy,' or not diverse enough. We question how we market information security as a place to work and consider what might be putting people off. Is it the language we use? Is it the imagery or colors? Perhaps it's the way the industry is portrayed in the media? I've heard all of the musings – I've often written about them.

We question whether it's too stressful as a career and whether the pressure we put on our CISOs and other industry professionals is a barrier to the industry's desirability. Are the hours too long, is the work-life balance (or lack thereof) unattractive? Perhaps it's about a lack of defined career paths or the inability to communicate them?

I'm aware I'm asking a lot of (rhetorical) questions. Bear with me, I'm a journalist, questions are what I do.

Ultimately, all of the aforementioned concerns are founded, but I do wonder whether the answer to solving the skills crisis lies more in introspection.

There has been no shortage of discussion around how we tackle, and challenge, the diversity problem. Whilst this has predominantly taken the form of dialogue around gender, there has been a heightened focus on ethnicity, neuro and disability diversity. *Infosecurity* is committed to reporting on, and supporting, diversity conversations and initiatives.

Brian's tweet highlights another issue, which is absolutely a contributing factor in our skills gap. Maybe the answer is looking at our own hiring practices and the – perhaps unreasonable and unnecessary – demands that we are applying when screening applicants. Brian specifically mentions a degree-level education and the discovery of CVEs, but these are only some of the demands hiring managers are making.

> ***"This is me arguing for a more open-minded, more inclusive recruitment strategy for the industry"***

The CVE point struck a chord with Brian's connections. "There are about 128,000 CVEs listed on http://mitre.org. Even at one per person that leaves us with a helluva skills gap!!!"(sic) replied @ChrisInfosec. Many other commenters wrote sarcastic affirmations that, they too, believe hiring managers in the sector are way too demanding.

Reducing – or even dropping completely – the requirement for formal education in specific topics, certifications or vulnerability discovery accolades may just open our eyes to a talent pool much greater. Before the cynics amongst you mutter anything like "Beggars can't be choosers" or "We're desperate, we need to be less picky," that's not the spirit in which this is intended. Nor is it true.

It's not about lowering our standards, it's about viewing excellence differently. How would academic acumen stand up against legitimate aptitude and passion? If I was hiring, I know what I'd prioritize. Clue: it doesn't cost anything and no dissertations would need to be written.

In the 14 years I've spent writing about information security, I've interviewed hundreds, if not thousands, of information security professionals. Of those, I can honestly say that about 40-50 of them have stood out to me as being exceptional. Exceptional at their jobs, exceptionally passionate about the cause and exceptionally loyal to the industry. I can think of only one or two of this group that had a formal education in the discipline. Almost without exception, they each regaled me with tales of how they "fell into the industry by accident," of how their passion grew organically or by coincidence. Not a single one credited a degree, a certificate or a CVE for their career or personal accolades.

This isn't me belittling the value of formal education, of CVE discovery or of industry certification. There's a lot to be said for all of them. Instead, this is me arguing for a more open-minded, more inclusive recruitment strategy for the industry generally. If we don't drop the barriers and open our minds, we've no-one to blame but ourselves when reading through the latest depressing skills shortage statistics.

I'll end this editorial as I began it, with Brian's words: "There is a gatekeeping mentality by some within the cybersecurity community to exclude people from entering the industry unless they meet specific criteria...as someone who does not have a formal third level education, nor any credits relating to any CVEs, I do find this gatekeeping mentality to be elitist and offensive and, to be frank, it has no place in today's industry." Well said, Mr Honan.

Enjoy the issue and take care

How to Master Modern Mobile Security

Arun Kothanath

Chief Security Strategist, Clango

Arun has more than 30 years of experience in information security architecture, identity management and fraud management systems. He has a CISSP certification and holds the honorary status of Oracle deputy CTO.

@Clango_Inc

Mobile devices are rapidly becoming part of every modern environment. The challenge is managing the ever-increasing demand for ease of access to information versus ensuring fail proof security governance. While regulatory requirements are still maturing, it is not enough to rely on complying with industry and federal regulations to keep your organization secure.

Mobile devices present unique vulnerabilities that demand different security strategies across multiple avenues of the device mobility spectrum, including mobile applications, content and identity.

In the new digital world, mobile devices are more than just another means to access information. These devices are perfect targets for attackers, since they are used for Multi-Factor Authentication (MFA) to critical applications and as a means for password-less authentication. Protecting the device must be a top priority. All mobile devices must have malware protection installed and access controls enabled. Additionally, enabling device-level biometric authentication measures will add a reliable safeguard against unauthorized access.

When enterprises deploy their own applications to their mobile workforce, all enterprise data protection aspects need to be considered. Data at rest and in transit should be subjected to the same data protection standards as any enterprise data. The ability to link company data to employee devices and ensure the data is secured and that overall integrity is preserved, is crucial. Encryption may seem like an obvious defense mechanism, but the application should adequately identify users' identity and privileges and enforce appropriate security controls. When APIs and micro services are used, data privacy must be guaranteed by enforcing authenticated standards.

The enterprise's mobile strategy should be to use Mobile Device Management (MDM) technologies that will incorporate visibility across the organization. Most often, enterprises are forced to support Bring Your Own Device (BYOD) policies, which complicate standardization. However, having an enterprise application store, enforcing encryption for enterprise data, enabling a 'find, lock and erase device' feature and blocking suspicious application installs will improve the overall security posture. Periodic mobile audits and penetration tests also rank high on the list of necessary cybersecurity activities.

In order to have a successful mobile security strategy, creating organization-wide awareness of mobile security is probably the most important action. Employees, along with anyone who is accessing the enterprise resources, should be knowledgeable regarding the risks of browsing, accessing data stores and enterprise applications, and the required security controls.

Organizations must also ensure that mobile devices are part of the enterprise identity and access management practices. A 'least privilege' strategy as defined by your organization's overarching data classification strategy will help to oversee mobile device security. Access certifications and entitlement governance should be part of the overall mobile security framework. In most cases, choosing an MDM capable of interfacing with an enterprise identity governance framework is highly recommended.

Consider a risk-based, continuous monitoring approach for mobile authentication. This approach will ensure continuous awareness of risk and will allow the organization to take appropriate actions based on context. However, this approach relies on the enterprise's understanding of its users, data and access patterns. It also relies on the ability to quickly react to potential policy violations.

In the digital world, a mobile device is part of an individual's identity. This makes defending the mobile device equally as important as protecting one's identity END

Anthony Di Bello

VP of Strategic Development, OpenText

Anthony leads a team of market development directors driving OpenText strategic direction within information security, data discovery, legal, analytics and AI/ML software markets.

@OpenText

Users today are digital nomads. Mobile and virtual, their devices (phones, tablets, notebooks, laptops, etc.) are everything to them. It's been over a decade since the practice of Bring Your Own Device (BYOD) became popular, and consumers now switch from personal, to public, to corporate networks automatically and seamlessly. With respect to access, they demand zero friction. Many in the tech industry have been talking about killing the password for years, but we are starting to see a real trend toward relying on mobile devices for what some call 'zero sign-on' access.

While employees and consumers have started to take a more proactive approach when it comes to cybersecurity over the past few years, there is still more that can be done around mobile devices. 2020 will be a key year for mobile device security given new demands being placed on these devices.

Organizations have enjoyed the multiple benefits of BYOD, and employees desire even more business functionality on their devices – but the implications for security are enormous. Fortunately, as the concept of the network perimeter has changed with the rapid adoption of cloud and mobile technologies, attitudes towards security have shifted. Businesses now realize that breaches – including breaches involving mobile devices – are inevitable. Businesses must embrace a solution that provides security without compromising privacy or functionality.

As the concept of a network perimeter further dissolves over the coming years, the enterprise especially will need to re-shape security strategy to account for the flexibility we are extending to our work force. It is time to acknowledge a simple fact: you can't protect what you can't see.

> ***"2020 will be a key year for mobile device security given new demands being placed on these devices"***

In particular, there are three challenges that must be overcome before organizations can be comfortable extending this kind of access control to mobile and wearable devices.

Visibility: unlike laptops and desktops, corporate IT does not have root-level access to mobile devices. BYOD devices are managed through Mobile Device Management (MDM) solutions restricting both business data and visibility into a virtual container on the device. For organizations to be confident in using these devices to broadcast a signal granting physical access, organizations will need hardware-level access to monitor the security of these components.

Privacy: as organizations look to gain hardware-level access to mobile devices in order to use them as access control devices, new measures need to be put in place to ensure the employee's personal activity is restricted from corporate view in a BYOD environment. GDPR, CCPA and similar mandates are the primary drivers for these requirements.

Control: this covers two things, the first being controls ensuring the person holding the device is the individual authorized for the access that device grants. This will likely involve a second factor, such as verification through the device camera before access is granted. Without the means to control and verify access at the device level, there will be additional risk in implementing this type of solution. Secondly, the organization will require an ability to deny access or shut down the device if the holder's identity cannot be verified END

Anurag Kahol

CTO and Co-Founder, Bitglass

Anurag co-founded Bitglass, a cloud access security broker, in 2013. As CTO, he is responsible for expediting Bitglass' technology direction and architecture. Prior to co-founding Bitglass, Anurag served as the director of engineering at Juniper Networks.

@bitglass

Cloud tools and applications are increasingly being used in the enterprise, enabling employees to better collaborate and increase overall efficiency. Additionally, bring your own device (BYOD) environments allow workers to operate from their preferred mobile devices and from anywhere with internet access, making it easier to share information and complete objectives. BYOD also leads to increased levels of employee satisfaction and reduces costs for organizations. However, the use of personal devices makes the management and security of the flow of corporate data more difficult. A recent Bitglass report on BYOD and security found that:

- One in five organizations lacks visibility into basic, native mobile apps on personal devices
- Only 56% of companies employ key functionality like remote wipe for removing sensitive data from endpoints
- 43% of organizations do not know if any BYOD or managed devices downloaded malware, indicating a significant lack of visibility
- 24% of organizations do not secure email on BYOD

Tools that are designed to protect managed devices do not translate well to securing personal devices, and unfortunately, some companies are hesitant to adopt BYOD for that reason. In fact, a recent study from Verizon found that 33% of organizations have suffered a breach through unmanaged devices.

BYOD environments change an organization's threat landscape and they require a different approach to security. Businesses must have a solution to mitigate the chances of data leakage, authenticate employees' identities, detect anomalous activity and address other mobile security threats as well. As a result, companies need to implement controls that enforce:

- Multi-factor authentication (MFA)
- Data loss prevention (DLP) tools
- User and entity behavior analytics (UEBA)

Mastering mobile security starts with the proper implementation of the aforementioned controls via an agentless solution that is deployed in the cloud. By leveraging an agentless solution, organizations will greater enhance overall employee mobility without the typical deployment, privacy or management obstacles that usually accompany both Mobile Device Management (MDM) and Mobile Application Management (MAM). This is due to the fact that employees will be required to have a software agent installed on their device with MDM and MAM, which yields control of that device to the organization and therefore controls how each worker uses their device, the apps that can be installed, and more. As such, this can hinder the overall user (employee) experience and even invade workers' privacy, as well as result in poor third-party and cloud app integration.

Fortunately, the availability of agentless, BYOD security solutions can address all of the issues associated with agents in MDM and MAM. In fact, agentless MDM solutions can help organizations control the flow of data, remain compliant, support cloud and third-party apps on any device, enable full visibility and audit, allow DLP from devices, and more without any software required. Therefore, organizations can have a robust foundation for keeping data secure in BYOD environments while being able to embrace the benefits of increased efficiency, reduced costs and improved levels of employee satisfaction END

FEATURE

THE DI
TRANSFORMAT

WHY SECU

IGITAL TION JOURNEY

RITY IS KEY

Kathryn Pick explores what the digital transformation journey can bring to an organization, and outlines why it's vital that security is at the forefront of innovations

If you want to have a modern day business ready to thrive, it has to be ready for the digital age. Digital transformation is being embraced by companies the world over as they seek to ensure every piece of process is modernized, and that the culture is embraced by staff and customers alike.

However, to get the recipe just right, security must be the key ingredient. So what can digital transformation bring to an organization, and what strategies must be implemented to make sure the journey is a safe, and secure, one?

What is Digital Transformation?

For Tom Rebbeck, research director at Analysys Mason, there is little agreement on the exact definition of digital transformation, but it is something that is broadly being looked at and embraced.

"For some companies, 'digital transformation' projects are just a cover for what is essentially cost-cutting," he argues. "For others though, there is a gradual transition to different ways of working."

This can include bigger moves into mobile technologies, looking to the cloud and taking on more automation. However, to make it successful, it has to be about more than just the tech.

Ruggero Contu, senior research director at Gartner, says: "It also involves the introduction of a new mindset requiring a constant rethinking of business approaches and how technology can support better services, and with that, improve competitiveness."

Also, of course, no company wants to be bottom of the pile. "There is an element of keeping up with the Jones' involved," says Nigel Ng, international vice-president for RSA Security. "If your rival is able to deliver a better customer experience, then they are likely to gain more market share."

Security's Part to Play

So, be it utilizing new tools, boosting your company's culture, or simply down to the brass tacks of outshining your competitors, it is clear why so many businesses are embarking on digital transformation journeys. However, what role does security have to play in this revolution of sorts?

Mike Nelson, vice-president of Internet of Things (IoT) security at DigiCert, celebrates the capabilities of the new technologies businesses are exploring – especially when they are mobile and connected – and lauds the improvements they can bring to companies and their customers.

"However, there is one big concern that must be addressed before we get too far down this path," he warns. "Anything connected is vulnerable to cyber-attack. With connected devices, these attacks could come in the form of personal data theft, device manipulation – think hijacking a medical device or mass outages of devices like security cameras – and other catastrophic events.

"Security must be part of the digital transformation journey to ensure consumers and businesses have confidence in the changes."

Ng from RSA agrees, adding that digital transformation projects are often customer-centric and data-driven, so security and regulation have to be key considerations.

"Unfortunately though, this isn't always the case," he says. "The focus on delivering new technologies before the competition can mean that speed takes precedence over security. Security teams are often seen as the 'no' people, who are always finding fault in, or trying to put the brakes on, innovation.

> ***"Security must be part of the digital transformation journey to ensure consumers and businesses have confidence in the changes"***

"This can lead to shortcuts being taken, with security teams being cut out of the loop, meaning insecure services and solutions can enter the marketplace."

The consequence of this can be dire – from the simpler frustrations of disruption or customer services being taken offline, through to reputational damage, or even the risk of huge regulatory fines that could have a major impact on business operations.

"So, ultimately, not having security functions involved in supporting the business throughout the process of digital transformation is often a false economy," adds Ng. "The time that might be saved in the early stages will come back 10-fold when the business has to deal with the ramifications of a breach."

Jeff Pollard, vice-president and principle analyst at Forrester sums up why security must be involved in one simple reason: "Security flaws can undermine the positive progress the firm makes with all its efforts, and cost it the ground it gained with employees and customers," he says.

Although, it is not just a case that certain C-level executives need to look at digital transformation from an overall business perspective – it is important for the infosec professional too.

"If you secure the way your firm makes money, then you make the security program vital to the company," says Pollard. "That's why things like product security and securing innovation efforts are so important as an initiative for security leaders."

In other words, it boosts the role of a security pro, and makes you a vital source that a firm may not have viewed you as before.

Staying Safe

So, we have established that digital transformation can bring big benefits, and that security has a major part to play, but how do businesses ensure digitization is done securely?

"From the ground up is probably the key point here," says Rebbeck. "Security is not something that can be added on later on top of other processes; it needs to be embedded into the new way of thinking.

"For each step of digital transformation, a business needs to think about how it can be built securely and how that security can be maintained."

Pollard agrees for the need of early markers, rather than later intervention. "Introduce the concept of minimum viable security as early as possible in the R&D, product management and development efforts," he says.

"Security and privacy by design need to be more than buzzwords, and the security team needs to adapt its approaches to work within chaotic and dynamic workflows."

Contu backs his peers, calling for the enthusiasm for each new technology to be matched by the enthusiasm for its security. "Businesses need to start with an assessment of the new risks being introduced by digital transformation," he says. "Then try to implement new processes and tools that focus on the most critical threats

and risks while enabling the business initiative undertaken."

Ng says, that to truly adopt a working digital risk management strategy when embarking on digital transformation, it has to be a business-wide effort and one that breaks down the barriers between IT, security and the wider workforce.

"To do this effectively, organizations need to combine smart technology, strong processes and employee education."

He says this is all dependent on building a workplace security culture that encourages greater security awareness. "The workforce needs to be educated and updated on the security threats and risks they will face in their job if they are to effectively recognize them and take the steps to manage digital risks effectively.

"An informed workforce can be the thin line between security and risk." He recommends company-wide training led by CIOs or CISOs which is made available to all staff.

Moves like this not only ensure that wider culture, and help users to do their job, but they engrain security as a key feature of any business venture into technology.

The Start of a Beautiful Friendship

These changes do mean there will be a lot of pressure on the security team to encourage the wider business to embrace them and perhaps closer scrutiny of their performance.

If you shine the spotlight on a previously shadowed part of the business, you have to make sure it highlights the best bits, but alongside this pressure, could digital transformation mean the relationship between a company and its security staff – and security leaders – flourishes rather than falters?

Rebbeck says it can, but it needs the backing of everyone at the top and for that to trickle down. "The leadership team of an organization has to understand and emphasize the importance of security as part of their transformation," he says. "Again, it is not as an afterthought, but embedded in processes, and not a one-off problem to be 'solved' but an ongoing initiative."

However, Rebbeck is confident such things are already happening. "The importance of security in a business has increased massively in the past few years," he says. "High-profile security breaches mean that security is no longer just an issue for the IT team, but something that boards are aware of and interested in."

The likelihood of someone in the business having seen articles about the Marriott hack, the attack on the NHS in the UK, or even having had their own email account compromised, is high. So, it is key to make the connection and show otherwise security blind employees how it plays into their work life, as well as their personal life.

Ng thinks it isn't just something to try from the top down either, but horizontally as well. "It comes down to the need to break down divisions within the business," he says. "It's often easy for different business functions to have their own ideas of what should be a priority, and this can lead to friction when priorities do not align, potentially raising business risk as a result.

"Instead of working as separate entities, IT, security and the wider organization must focus on communicating with each other and working towards shared goals."

Digital transformation could be the project that brings that opportunity. "It offers the chance for company-wide communication and for the streamlining of efforts towards securing the business," he adds. "In this way, security will no longer be side-lined as a task for just the IT teams, and instead will be adopted as a shared responsibility across the entire business."

Although, it isn't all on the other employees to embrace security, it is security teams that will have to build on their ability to reach out as well. Contu says: "As a result of the new pressures in place, security is required to improve its relationship with business by aligning and supporting digital transformation rather than trying to block initiatives for the sake of security.

"The relationship can improve through an improvement in the way security communicates the board/management and, on the other hand, the business' better understanding of the new security risks and support of the security efforts to tackle those risks."

> ***"The leadership team of an organization has to understand and emphasize the importance of security as part of their transformation"***

Digital transformation is an exciting, opportunity-filled move for any company to make, and if security is at the top of the agenda, it can become a real success for business. It is also a chance for security professionals to show their skills, their worth and build a broader culture in a company where they are not the underappreciated team that says 'no' – they are the forward-thinking team paramount to building a business END

TOP TEN Worst Vulnerabilities

01
MS17-010 (Eternal Blue)

Part of the most costly attacks in history so far, WannaCry and NotPetya both used Eternal Blue-style attacks as part of their payloads.
Source: Microsoft

02
MS14-068

This could allow an attacker to exploit a vulnerability in Microsoft Kerberos and elevate unprivileged domain user account privileges.
Source: Rapid7

03
CVE-2019-0708 (BlueKeep)

Despite multiple warnings, it took until November 2019 for the first exploits of Bluekeep to be spotted. It has been predicted that a widespread exploit could be severe.
Source: Fortinet

04
MS08-067 (Conficker)

This Windows SMB vulnerability is over 10-years-old, and still seen in older networks with legacy gear.
Source: SANS Institute

DAN RAYWOOD

Top Ten Worst Vulnerabilities

Vulnerabilities proved to be one of the main security trends of 2019. Despite all of the testing, warnings and advice around vulnerability management, it seems the challenges that organizations face in finding and patching vulnerabilities are not going away anytime soon.

Industry research shows that the number of unpatched vulnerabilities continues to increase, stating that patching is typically delayed by 12 days due to staffing issues, while 72% of security professionals surveyed by ServiceNow reported difficulty in prioritizing what needs to be patched.

With this in mind, and to highlight the risks of unfixed exploits, *Infosecurity* has compiled a list of 10 of the most infamous, troublesome and damaging vulnerabilities faced by businesses across the world in recent years.

05
MS01-023 (Nimda)

Nimda was a package of Microsoft IIS exploits that were released a week after the 9/11 attacks.
Source: Microsoft

06
Spectre/Meltdown

These speculative execution bugs were unexpected and drove new areas of hardware security, proving that CPU security was still important.
Source: Meltdown Attack

07
CVE-2014-0160 (Heartbleed)

Heartbleed is a vulnerability in the OpenSSL code that handles the Heartbeat extension for TLS/DTLS.
Source: Synopsys

08
CVE-2008-1447 (Kaminsky Bug)

This DNS vulnerability allowed attackers to send users to malicious sites and impersonate any legitimate website and steal data.
Source: Duo Security

09
CVE-2014-6271 (Shellshock)

The remote code execution vulnerability affected Bash, and could allow an attacker to gain control over a targeted computer if exploited successfully.
Source: Symantec

10
MS02-039 (SQL Slammer)

MS02-039 hit on the weekend of 25-26 January 2003, causing a denial of service on some internet hosts and dramatically slowing down general internet traffic.
Source: ESET We Live Security


Outpost24
Outpost24
Outpost24
Outpost24
Outpost24
Wendy Nather

Michael Hill meets the fabulous Wendy Nather, a woman whose love for security is inspired by her passion for new adventures and tackling the next big challenge

WENDY NATHER

There aren't many people in the security industry that are more fascinating or more delightful to meet than Wendy Nather. She's known the world over for her knowledge, insight, thought-leadership and, perhaps above all, her wonderful sense of humor and willingness to give anything a go (I'll never forget seeing Wendy singing her heart out onstage as part of a security choir at RSA 2019!).

She is quite the inspiration, not just because she's led an amazing career in the tech industry that has seen her fulfill various roles in both the private and public sectors, but also because she's overcome challenges and difficulties that many of us can only begin to imagine being faced with.

I, like many others in our industry, will always have a real soft spot for Wendy – she's always been warm and welcoming to me personally, and has also been an invaluable source of support and knowledge for *Infosecurity* Magazine for many years. She will probably be slightly bashful when I say it, but she really is one of a kind, with one hell of story – and it's high time we tell it!

Wendy's career has steered her to her current role of head of advisory CISOs at Duo Security (now part of Cisco), but she reflects that, long before she took even her earliest steps in the tech industry, it was the extraordinary occupations, talent and life of her father that had a big influence on her own trajectories.

"My father was an English Major in college, and he ended up becoming a nuclear physicist," she says. "Well, originally he wanted to be a science fiction writer. When he was doing research for a book idea he had, he was talking to the director of a nuclear facility. The director told my father: 'you know, you can be a nuclear physicist and you can write science fiction in your spare time, but you really can't do it the other way around' – and so he offered my father a job."

That man's name was Charles Wende – "I found out later, that's where my name came from," Wendy says with a smile. "It wasn't from Peter Pan! My mother may have thought it was, but it was actually in honor of this man who gave my dad a job as a nuclear physicist, just out of the blue."

Wendy's father, Ed, does sound like quite the intriguing individual. He wrote one of the very first FORTRAN compilers, and based on his work in early computing, wrote *The Story of Mel* (a tale about the beauty of programming that went viral in the early 1980s and is still available on the internet today). He invented a lab machine that featured in the opening credits of the movie *Fantastic Voyage*, before waking up one day in his 40s and deciding he wanted to become an astronomer – which he also went on to do.

"He was successful going from job to job, in various different places, with little formal training," Wendy explains – a trait, as you'll soon learn, Wendy would inherit herself. Wendy's father also introduced her to her first computer when she was 12 and the family was living in Tel Aviv, Israel (this is after stays in both Austin, Texas and Cape Town, South Africa), all places in which Wendy's father worked and explored various academic pursuits.

"It was he that taught me programming," Wendy explains. "I had told him I was bored – which is a mistake, you should never tell your parents you are bored," she laughs. "He gave me this book and told me write a program that would make the bell on the teletype ring. He taught me that really to just give me something to do."

A Language Lover

It wasn't just a proficiency in programming that Wendy would develop though. Thanks to her father's jobs being located in some pretty exotic places, she was able to learn some Afrikaans while living in South Africa, and some Hebrew while living in Israel. "I became very interested in foreign languages," Wendy says. "In high school I took German, French and a little bit of Russian. I majored in Liberal Arts in College [University of Texas], concentrating on languages and history, spending my junior year abroad at the University of Würzburg, in Germany."

By my count, that's five different languages (six if you count English) learned whilst living in four different countries – all by the time Wendy was in her early-20s. That's impressive stuff! So what led Wendy to the technology sector when she had such a passion and aptitude for foreign language?

Again, her father played an integral part, setting her up with an account on a PDP11 minicomputer when she was at university. "That's when I learned Unix and I used its nroff and troff utilities to write my papers," Wendy explains. "At that time, you usually had to type everything out and if you made a mistake, you'd have to go back and start the page again. For me, being able to type everything up, format it nicely and print it out, it felt like cheating! I became very good at formatting languages and I got jobs helping other people format papers whilst I was at college."

Wendy found that the job offers, and the money, kept coming, so she made the decision to drop out of university and enter the full-time working world.

A Rolling Stone

Wendy moved to Indiana and worked as a typist and formatter before taking a job in New Jersey as a technical writer for Unipress, a software company, where she documented Gosling Emacs. She then headed to Virginia and found work at an interactive videodisc startup, in 1986. Are you keeping up? Good – because Wendy was soon on the

move again a year later. This was when "things really started to come together," Wendy tells me.

"I moved to Chicago and I was working as a technical writer and system administrator at a private options trading firm called O'Connor and Associates," Wendy says. "They announced they were being acquired by Swiss Bank Corporation – which at the time was the second or third largest Swiss bank. I knew German and French [both widely spoken in Switzerland], and Unix. Suddenly these three things came together in a way that I did not anticipate. They needed somebody, located in Zurich, to help deploy and manage the trading infrastructure they acquired us for. I spoke German, I spoke French, and I knew the technology, so I volunteered to move to Zurich."

> ***"I think there are probably few people who have stayed as much of a generalist as I have"***

Wendy lived and worked there for three years, managing the Unix systems O'Connor and Associates deployed to Swiss Bank as part of the takeover. "I never would have thought that my Liberal Arts education and my languages would have come in handy, together with the computer work I was doing, but it just serendipitously became a natural fit."

When the company decided to outsource its IT operations in 1995, Wendy was put on a task force to figure out how that could be done without violating Swiss banking laws. "The company then sent me to London to head up the security team for the EMEA investment banking division – and that's how I got into security."

Wendy smiles as she tells me how much she enjoyed spending two years in London. "I had a very well-appointed 'broom closet' in Chelsea!" she laughs. She headed back to Chicago after that two-year spell to work as part of the global security team, before taking some time off work and moving back to Austin to care for her parents and have the second of her two children.

Wendy's love for foreign languages and aptitude for programming have led her to the information security industry

A Public Servant

After that time of hiatus, Wendy's career journey took another new turn when she began working at the Texas Education Agency, overseeing its security program. "That was very different from Swiss Bank," she explains. "When I was at Swiss Bank, I was helping to manage a budget of around $50m. On my first day at the Texas Education Agency, I walked in, and I was the only security person, and they wanted my budget request by the end of the day. I asked for a logging server and a couple of books – like $2000 – well, the person I was reporting into scribbled it out and said 'where do you think you are, the private sector?' – so I had a budget of zero and zero people when I started there."

That must have been quite an experience, and Wendy recalls that her five years at the Education Agency taught her a great deal about security. "The attitudes towards security were very different. Back then it was difficult to make the case [of the importance of security] in the public sector. Luckily, I ended up with a new CIO who very much appreciated the need for security. He supported me and got me the people and budget that I needed."

That's where Wendy got her appreciation for companies that are below what she calls "the security poverty line." There are certain things that they simply can't do, she says, "and it's not just a matter of giving them free software. There are a lot of other dynamics involved in that kind of poverty and the constraints that you're under in the public sector."

You have to be very creative; you have to borrow, beg and barter, Wendy says fervently. "You do whatever you can to put in as much security as possible, regardless of whether you have budget for it or not."

Wendy clearly developed a real passion for working to make the public sector more secure, and her decision to leave the Education Agency in 2010 was no doubt a difficult one to make. "I was talking with Nick Selby, who founded the security practice at 451 Research," she says. "I'd gotten to know him through Twitter, and we were hanging out at a conference in Dallas. He turned to me and said 'why don't you think about becoming an industry analyst?' I initially thought I wouldn't be able to do that, but Nick said 'well you have the practitioner experience, why don't you give it a try!' By that time I had met Josh Corman [also originally of 451 Research] and he hired me into his team, as an analyst."

So once again, Wendy embarked on a new position, with new challenges and new goals. I do truly admire not only Wendy's ability to keep doing that, but also her fearlessness to do it. Nonetheless, I also can't help but ask if there's a reason why she's moved around quite so much?

A Fearless Fighter

"Well," she says, "in my forties I was diagnosed with attention deficit hyperactivity disorder (ADHD), which explains why I always bounced from one thing, to another thing, and why I was really happiest when I could switch jobs, countries and states. I was always looking for the next challenge or the next opportunity."

Ah! That does go a long way to explaining her tendency to constantly be on the move, although it's a real credit to Wendy that she's been able to use her condition to her advantage and experience a wealth of different jobs and opportunities. However, ADHD would prove to be only one of the conditions that had a big impact on her life.

Unfortunately, in 2011 and after she took over as director of the security practice at 451 Research, Wendy was diagnosed with breast cancer. A tough diagnosis to say the least, but Wendy was determined to forge ahead in her work.

"I continued to work, and I was really worried that if people in the industry or our research customers found out that I was ill, they would lose confidence in me, in my team and in the company" she says.

"I didn't tell most people – some friends knew," Wendy says, and she reflects on how she would sometimes work from her bed throughout her treatment, which continued into 2012. "There were a lot of medical emergencies during that time," she adds. "The treatment itself made me very sick, and there were times when I ended up in the hospital for a few weeks."

Wendy was pronounced to be in remission in 2012 and was able to go back to working and travelling with 451 Research full-time, something that came as a huge relief to her, but also saw her faced with ongoing challenges that still affect her today. "The thing with chemotherapy is that it leaves a very long tail – it affects your body far after it's done. For example, I developed rheumatoid arthritis, which is something that can happen with the therapies. Chemotherapy resets your immune system, and I spent the next several years dealing with the lasting effects of chemotherapy; I'm still dealing with those."

She faced those difficulties head-on though, also continuing to care for her parents through their own periods of ill health until they passed away in 2014 and 2015, and raising her two children. She was lead of the security practice at 451 Research until (yep, you guessed it) she took on a new challenge once more. She joined the Retail ISAC (now called the Retail and Hospitality ISAC), which was just launching in Austin in 2015, and led the company's research team.

> ***"I have no idea where I'm going to end up, but I'm enjoying the waves"***

It was while Wendy was in this role that Duo Security invited her to its newly opened office in Austin, in 2016. "I had gotten to know Duo whilst I was at 451 Research, alongside all the other security companies," she explains. "As soon as I saw Duo's product, I thought wow this is amazing!" she says. "I got to know Dug Song and Jon Oberheide [Duo Security's founders] and I really liked their vision. They had invited me to come and speak at one of the Tech Talks they were hosting. I came into the office there, I met the people and I really loved the atmosphere. So, I said, 'would you happen to have any room for me at Duo?' – it turns out they did! So that's how I came to join Duo," Wendy beams. "Now that Duo has been acquired by Cisco, it's like having a whole new job all over again!"

Wow – so that, if you like, is Wendy's career journey (so far) in a nutshell. It's been a whirlwind (to say the least), and I wonder, having achieved so much in so many different roles in so many different places, what Wendy is most proud of in her career?

A Wave-Riding Surfer

She ponders for a few moments. "I think there are probably few people who have stayed as much of a generalist as I have," she says. "Usually, people will pick a specialty and go very deep into it. I've tended to go as deep as I've needed to at the time to learn something about a technology, especially so that I could write about it as an analyst. So going both deep and wide is something that not too many people do anymore."

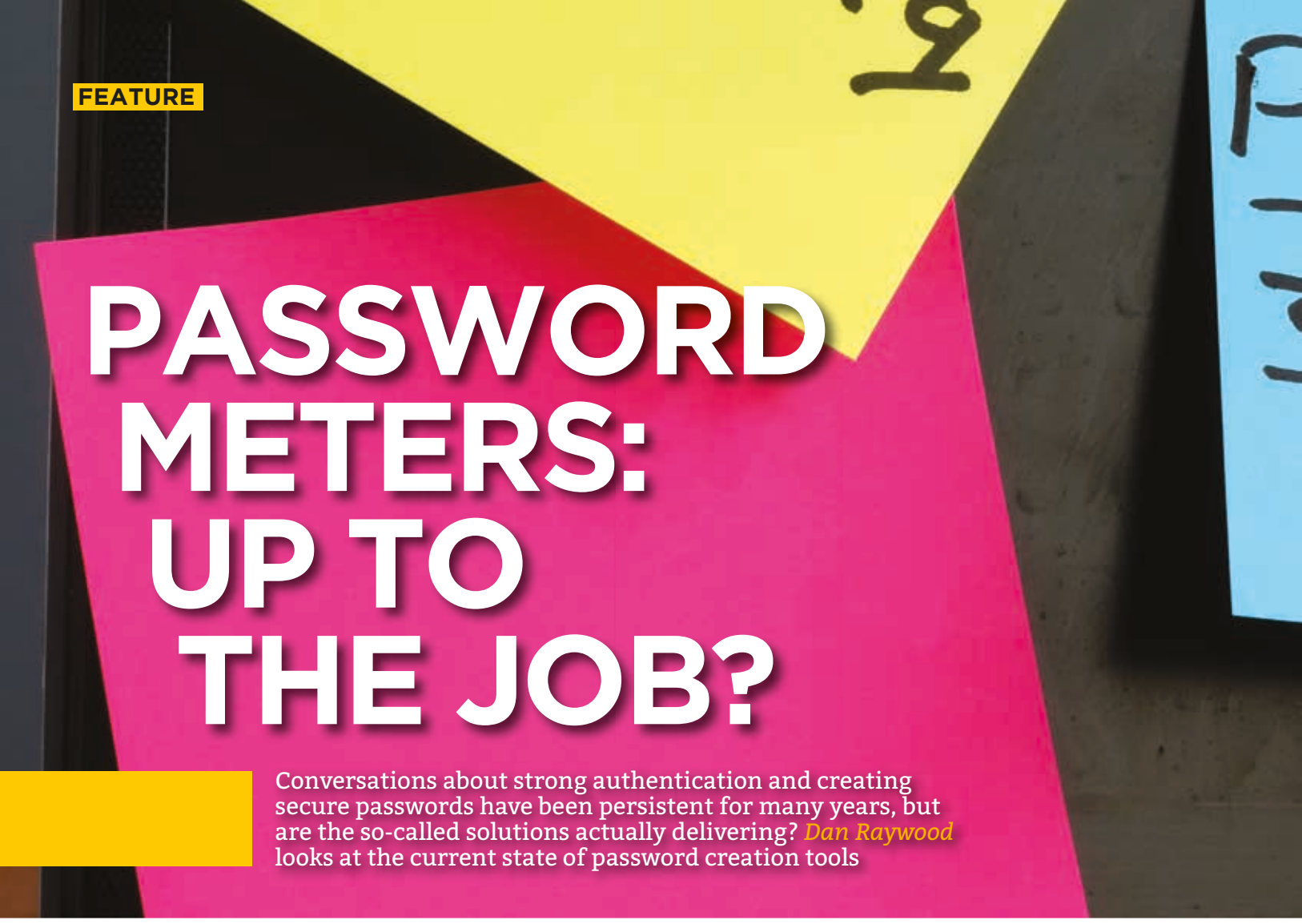
So, no regrets? I ask. Again, Wendy takes a few minutes to think her answer over. "I think that, in some ways, people have regrets if they have a goal that they were working towards, and if they do something that doesn't get them closer to their goal, it becomes a regret. However, since I didn't have a goal, I actually don't have those sorts of regrets.

"I admire people that have a goal and they work towards it – they pick a spot on the horizon and they just steer towards it and nothing will get in their way – but I'm more like a surfer. I'll look at the waves and think 'hey, that one looks good,' and then when it peters out, 'hey there's another one coming along, let's take that one.' I have no idea where I'm going to end up, but I'm enjoying the waves!"

That's why she's found security such a fulfilling career, Wendy adds, because "there's always something new to learn. Either in the technology itself or in the application of security. It is very intellectually challenging, and there's a huge difference between theoretical security and applied security. So much of the challenge is figuring out how to make the theoretical solution work in a real environment. That's both the challenge for me, and the frustration. I love hearing stories of how people have been able to do that."

There are so many different ways to view security, she adds, "so if I ever get bored of looking out of one window, I can go look out another window."

I think whichever way you look at it, the security industry would not be the same without Wendy Nather! END



FEATURE

PASSWORD METERS: UP TO THE JOB?

Conversations about strong authentication and creating secure passwords have been persistent for many years, but are the so-called solutions actually delivering? *Dan Raywood* looks at the current state of password creation tools

In November 2019, it was revealed that Italian bank Fineco Bank had suggested that to test the strength of your password, try entering it into a search engine and "if it returns less than 10 results, it means it's a good password."

According to *Vice*, Fineco Bank customer support confirmed that the bank suggests customers Google their password in order to make the password "as secure as possible." A comment request by the publication later found that the policy had been scrapped, with a spokesperson saying "we understand the criticism and we decided not to suggest…our clients do so anymore." This was not before widespread criticism of the practice on social media though, with one person suggesting it could be an early April Fool's joke.

Are You Confused?

This led *Infosecurity* to question what the best practice for building a decent standard of password is. Research on password security is plentiful: a survey of 1000 adults in the UK by PCIPal found that 26% use the same password for multiple websites. Research by HYPR of 200 people found that 72% of users reused the same passwords in their work and personal life, and 49% admitted that when forced to update their passwords in the workplace, they reused the same one with a minor change.

Also consider that on average, 12.6 minutes each week - or 10.9 hours per year – is spent entering and/or resetting passwords. Research by the Ponemon Institute and Yubico found that for a company with a headcount of 15,000, the annual cost of productivity and labor loss per company averages $5.2m annually.

People and employees will look for the easiest option around a problem, that's well known, but with evidence showing that they will find a way around password security, are we confusing the public by insisting they need to be more secure online, but providing very unclear advice on how to do so?

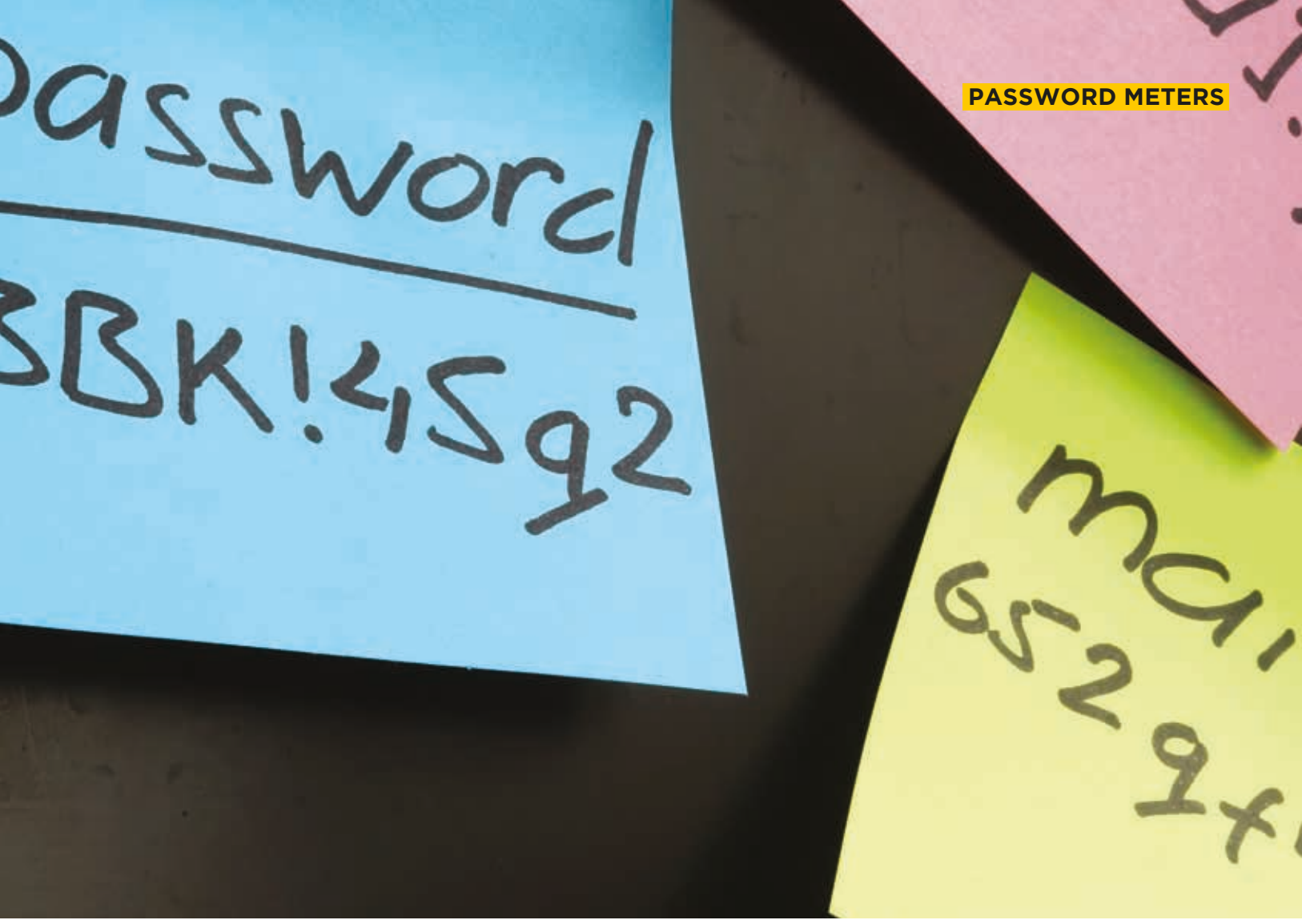
Inconsistencies and Incompetence

In October 2019, *Infosecurity* was invited to participate in the Secure South West conference, held at Plymouth University, where Steven Furnell, associate dean for International and Postgraduate Faculty of Science and Engineering, presented new research around the problems of creating a secure password.

His research involved running the most commonly used passwords against password meters, to see which would determine the password to be good, acceptable or bad. Furnell says that the research found the meters to often be "totally misleading," as the method for determining how good a password is was based on lower and upper characters and symbols. "However, that doesn't reflect how you choose a password," Furnell warns.

The experiment involved 16 password meters, which included 10 dedicated meter sites, five that were in popular online services and one from a standard operating system. The passwords tested included 10 that were explicitly weak and ranked in 'common password' lists, two that were theoretically OK, but practically not – as they fit the standards of a mixture of upper and lower case characters and special characters – and four passwords that ought to be regarded as sound choices.

The research showed that the main 10 weak passwords were mostly rated as 'poor' or 'weak', however because of the combination of letters, special characters and numbers, the infamous 'Password1!' was actually classified as 'reasonable' and 'good' by two of the meters.



There were inconsistencies and conflicting results amongst the research. A classically perceived stronger password, in this case the combination of three random words, 'donkeykansasburger' was rated as weak by three of the tests, but also 'strong', 'excellent' and 'good' by three others.

Furnell explains that the reason for choosing 'donkeykansasburger' is because the three words in isolation would appear in a list of typical worst passwords, but put together as one string, they appear to be a stronger password. However in another experiment, three other random words 'wretchgravelgeese' was consistently rated as strong.

Furnell says that of the 10 explicitly weak passwords, only five were consistently scored as weak by all 16 meters.

In addition to finding that a bad password could be deemed good, Furnell also discovered that four of the 16 meters that he tested provided upfront guidance when making a selection, and only five provided feedback on how to improve it.

With regard to the meters offering guidance and feedback, Furnell says that if you are providing a password meter, you need to provide guidance of what 'good' looks like. "The guidance may be as simple as a list of common passwords, or [a suggestion] to pick three random words."

If a password is determined to be 'poor', Furnell questions what the person is supposed to do about it. "The websites should consider that they are dealing with people, and surely the role of the password meter is to help them do it well. If you provide them with guidance and still let them use [the meter] blindly, it is not going to lead them out of the problem."

With 'Password1!' rated as moderate by three meters and 'good' by three further meters, what does this tell us about the effectiveness or accuracy of password meters? Furnell says that the whole point of the technology is to encourage users to do things "right or better, but if they are all behaving in a significantly inconsistent manner, then it ultimately comes down to which meter you choose as to whether you may or may not end up with a good password as a result."

The issue is that they all seem to play by different rules, he says, and while some of them are created by commercial companies who can sell a product related to authentication, the best test of a meter's worth is to have a baseline password test. "Try something like 'Password1!' and if the meter gives you anything but weak, walk away," he says. "All of the other weak passwords didn't get anywhere near the level of acceptance that one did. If it gets rejected, the meter is probably baseline sensible."

To Insist or Not to Insist?

All of this raises the question of how the industry can enable the public to create and use stronger passwords. Furnell says that we can "chastise and complain about user actions as much as we like, but if we are not doing the baseline stuff to actually help them, what do we expect?"

Is it actually possible to insist on 'strong' passwords being used? Ed Tucker, co-founder of Human Firewall and Email Auth, says that doing such a reset with a demand for 'strong' passwords whilst rejecting anything deemed to be weak is very hard, and it is easy to annoy people. "It can encourage bad habits like 'Winter2019!'" he says. "It only really works with helpful guidance that explains why it is a good thing for their home life as well as work life, and advice on how to make it simple."

Tucker also says that engagement is key. "If you speak in a language that the user understands, rather than some prejudiced security verbiage, you bring together an

understanding of why password strength is important in users' personal lives," and this can help them develop a culture that they can employ outside of work to better protect themselves.

He recommends a strategy of "making complex simple" by engaging with the user, and by helping them understand common pitfalls like capitalizing the first letter "and how to overcome this without bamboozling them."

On an *Infosecurity* webinar held in December, a poll question asked: 'Is it possible to insist on a policy of 'strong' passwords?' The results showed that of those who voted, 92% said that it was possible. Sarb Sembhi, CISO of Virtually Informed and co-founder of Security2Live, who participated in the webinar, says that it is only possible to insist on this policy if you provide the tools, "because most people have around 50 passwords and if you expect people to have a strong password, you need to provide a tool to enable them."

He says: "The bottom line is that in some respects everyone who works for an organization, small or big, they are there to do the job that they are trying to do and want to do it in as quick a way as possible and focus their attention on getting the work done, not trying to remember passwords. No matter what tool it is for authentication, you have to make it easier [to use] and only then can you insist."

Is the Industry Responding?

All of this advice on how to build a secure password does lead us to consider what is being done to actually inform the user when they are using a 'bad' password. A number of browser extensions have been introduced over recent months to inform the user when the password they are using has been caught up in a breach.

A recent introduction to version M79 of Google's Chrome browser will inform you if your password has been involved in a breach, with a suggestion that the user changes their login information. This is done by turning the password into a hash and turning it into an undecipherable string of numbers and letters. If the same password exists in Google's archive of previously stolen logins, a matching hash will be found to avoid comparing plain text passwords.

Another option is the browser plug-in Shield from OneLogin. The company says that this works by "taking a hash and comparing it with known hashes and looking for comparisons." Currently available as both a free and paid for product, Kayla Gesek, product manager for Shield at OneLogin says that the plug-in flashes up an alert when a password is used from a list of commonly breached and used passwords, and settings allow the user to see where a password is being reused.

She says that reuse is the main intention of Shield and prevents password reuse, but will also alert a user to when a weak password is being used. "It really doesn't do you any good if you have a long and difficult-to-crack password but are reusing it everywhere. The one time it gets cracked the hacker has access to every account that you are using it on," she says. "The reuse factor is a bigger issue than the complexity problem."

The focus has shifted more to reuse and preventing the issues associated with account takeover that lead to phishing and business email compromise. Over the past 10 years we have had many conversations about password security and replacing them with an alternative, but as we enter a new decade, it seems that passwords are the only viable option for widespread authentication.

> ***"It really doesn't do you any good if you have a long and difficult-to-crack password but are reusing it everywhere"***

The reality of creating a strong and secure password remains uncomplicated, but actually getting the message out is as much of a challenge as creating a secure, strong and unique password for every login. If, as Steven Furnell's research shows, even the tools designed to help people cannot be totally relied upon, will we still be having the same conversations in 10 years' time? END

What is a Password Meter?

Featured on many websites, and also as a feature by many password managers and IAM technology, password meters give you an idea of how strong your password is. Steven Furnell says that they "aim to give an indication of the suitability of users' password choices" and attempt to "nudge them towards better behavior" by sometimes offering advice on how to create a more secure password.

The website passwordmeter.com states that the application "is designed to assess the strength of password strings," however it does claim that it "should only be utilized as a loose guide in determining methods for improving password creation."

Q&A

STEVE DURBIN

Steve Durbin is a senior security leader at the Information Security Forum (ISF) with a diverse background in both business and technology. He has managed and grown startups to multimillion dollar turnover technology and services enterprises, and been involved with mergers and acquisitions of fast-growth companies across Europe and the USA. Although his career has led him to the information security industry, he graduated with a degree in French and studied for his Chartered Institute of Marketing qualifications before moving into the working world

By Michael Hill

What was your route into the information security industry?

I came into security purely by chance after having been offered the opportunity of working with another industry leader, the late Howard Schmidt, special adviser for cyber space security for the Bush White House, directly following the 9/11 attacks. Howard was the president of the ISF at that time, and the opportunity was to help with the growth of the ISF by introducing new services and member offerings to meet the continually evolving needs of our members. I now oversee the ongoing development of the ISF worldwide. I also sit on the ISF board and so have first-hand input into our strategy and ways of dealing with the ever-complex business world in which we operate.

What's the best thing about your job?

My job takes me to many interesting locations and I get to share views and ideas with some of the brightest people in the world. However, the best thing about my job is the people; the ISF continues to grow, and in our business that means we need to attract and retain people who both enjoy the challenge of working in a fast paced, dynamic industry and are able to hold the attention and respect of our members. Security is a people business and to be effective we need to create a shared vision for our people that they buy into and support.

What would be your dream security project, and why?

My dream project would be one that looks at the geopolitical impact of cyber over the next 10 years. As I have frequently stated, the battle for leadership in next generation technologies is steadily growing and this is currently manifesting itself in the beginnings of a potentially globally damaging US/China trade war. For me, the ways in which cyber and the associated implications of cybersecurity and privacy develop through AI, cloud, smart cities and the IoT will have a significant impact on everyone's lives. It would seem timely to look at the geopolitical issues related to cyber and cybersecurity in this context.

What's the most interesting thing about information security?

It never stands still! It is continually evolving and changing and to be effective we, at the ISF, and our members in their companies, need to be constantly bringing our 'A game' to combat the increase in threats and risks.

What would you change about the security industry?

I would like to see more focus on the role of the individual and greater understanding of the people element of security. All too often, we jump to technology or processes as a means of enabling or ensuring security and miss that people have the ability to be the strongest link in any security chain.

Quick-fire Q&A

What did you want to be when you were growing up?
An airline pilot.

What's your favorite film?
Apollo 13.

What's your guilty pleasure?
Single malt whisky – I'm a collector (or a hoarder as my wife would say)

BIO

@stevedurbin

Steve Durbin is managing director of the Information Security Forum. His main areas of focus include strategy, information technology, cybersecurity, digitalization and the emerging security threat landscape. Previously, he was senior vice-president at Gartner.

TWO EXPERTS GO HEAD TO HEAD

Point

Compliance Competency: Improving Security

Brian Honan

Owner, BH Consulting
Brian is an internationally-recognized expert on cybersecurity. He has acted as a special advisor to Europol's Cybercrime Centre (EC3), is head of Ireland's CSIRT and has been inducted into the Infosecurity Group Hall of Fame.
@BrianHonan

Anyone familiar with the Monty Python movie *Life of Brian* can no doubt recall the famous "What have the Romans ever done for us?" scene. In this scene, the activist group Brian has joined is looking to overthrow Roman rule. In a conversation where the people in the group lament the ills the Roman Empire has inflicted on them they also highlight the advantages, such as roads, aqueducts and law and order, which Roman rule brought to the region.

In many ways, this scene reminds me of the cybersecurity industry which regularly laments how ineffective security controls are implemented in organizations and yet, at the same time, doesn't appreciate the benefits that cybersecurity standards and regulations have brought.

If we look at key turning points in recent times resulting in boards and senior management focusing more on cybersecurity, I argue it is the introduction of security standards and regulations that have driven this new focus. This, coupled with the increasing reliance all businesses and organizations place on technology and the sharp uptake in the number of very public security breaches, has made many companies look towards their security for reassurances that their organization will not be the next to hit the headlines for all the wrong reasons.

The traditional response from many security teams has been along the lines of "trust us, we know what we're doing," but I would argue that this is no longer an acceptable response. As with every other aspect of business, be it HR, health and safety or finance, there are standards and regulations which those business functions have to comply with.

The introduction of the EU General Data Protection Regulation (GDPR) has introduced more stringent penalties for businesses failing to secure the personal data entrusted to them by individuals or for not honoring their rights. There are other regulations the EU has introduced which have not garnered the same attention, such as the EU Network Information Security Directive, focusing on organizations providing essential services and critical infrastructure, the Payment Services Directive II for improving the online security payments environment and, during the summer of 2019, the EU Cyber Security Act also came into force. The Cyber Security Act paves the way for the EU to introduce certification schemes to certify products and services, particularly in the Internet of Things space, as being secure. Other jurisdictions are looking at how Europe is regulating the security industry with a view to introducing similar regulations. We also see different industry sectors, particularly those that are regulated, looking to introduce ways to ensure organizations within their sectors are implementing an acceptable baseline of security.

> ***"Standards provide the security team with the opportunity to engage with the business"***

The argument often cited against standards and regulations is that security teams and businesses will not focus on properly securing their systems, but rather do the bare minimum to comply with the relevant standards. This may have been true in the past, but in my opinion, this is rapidly changing. The key reason I say this is because many of the above regulations now hold organizations – and indeed in some cases (such as the GDPR) individuals within those organizations – responsible and accountable for not ensuring the security of their data or services.

This focus on holding organizations accountable has taken cybersecurity out of the realm of the IT and the security teams and placed it firmly in the hands of the risk committees, audit committees and the board. In order to manage the risk associated with this accountability, many organizations will now look to those responsible for security not only in their organization, but also with any third-party providers they engage with, to demonstrate to them that they are implementing recognized industry good practices in securing their data. Hence we are seeing a drive towards many organizations looking to get certified to the ISO 27001 Information Security Standard, or for smaller firms, seeking certification through the Cyber Essentials scheme.

This move towards standards is not only driven by the businesses themselves, but in order to offset the risk associated with a cybersecurity breach, organizations are looking towards cyber insurance. In turn, cyber insurance companies are looking at their clients and asking them to demonstrate the measures in place to manage their cyber-risks, adhering to a recognized standard that can satisfy that requirement.

So if we were to look at the 'Cyber Life of Brian,' we should not lament the paperwork and governance overhead that standards and regulations bring. Instead we should recognize that not only do standards require a minimum baseline for all to adhere to, but also provide the security team with the opportunity to engage with the business and get the support needed to implement security in a positive way

Counter-Point

Strategies vs Far From a Security Guarantee

Compliance does not guarantee security. Security leaders in regulated industries understand this mantra, however historical breach trends are beginning to show that compliance-focused security programs aren't doing enough. Verizon's 2019 *Data Breach Investigation Report* examined 41,686 security incidents and 2013 data breaches across 86 countries alone, highlighting the fact that cyber-attacks continue to happen, and threat actors continue to circumvent the defensive measures put in place by enterprise security teams.

There is a multifaceted hypothesis for this trend; organizations do important work and are consequently always attacked and there are several requirements companies must adhere to that creates ambiguity. However, threats stemming from regulatory roots have created opportunities for organizations to treat compliance as a foundation for their security programs.

Regulated industries require oversight as assurance. National and global critical infrastructure organizations need excellent oversight due to the importance of the work they do. In fact, a recent Ponemon Institute study found that 90% of national infrastructure operators had been hit by at least one successful cyber-attack. In today's technology-enabled age, cybersecurity regulation sets the minimum bar of security requirements.

Regulations that are born from local, state, national and international legal remits are not always impactful in addressing emerging threats surrounding modern computing methods, and result in several nuanced mandates for businesses to adhere to. The onus is on the company to navigate which regulatory rules apply to them. However, engaging in domestic and international business creates a complex equation of what data protection and privacy regulations apply. From this difficulty arises confusion, and confusion results in error, all to the advantage of cyber-attackers.

Industry has appropriately responded to help companies that are affected by the complexity described above. Several consultative firms have emerged to help on both sides of the fence of the compliance equation. They work with the regulators to support the compliance verification and audit processes, laying out the rubric of assessment, or serving as labor to execute the interviews and data collection of the audits. They also help businesses prepare for these audits by outsourcing the preparation, or driving 'mock audits' as readiness exercises.

> ***"One of the biggest issues with current regulations is the periodic nature of compliance assertions"***

These challenges result in an often significant security expenditure in navigating regulatory hurdles, which drains resources for broader security investments, also known as the security investment Solomon conundrum.

Some of the most defined and specific regulations applied to some of the biggest breaches we have seen in recent history, but the climate is changing. The incentives to do more just haven't been meaningful and, due to the periodicity of updates, most breaches that have occurred have been within compliant organizations. For example, in December 2013, it became publicly known that Target Corporation was breached and 110 million consumers' payment card information, names, phone numbers, email and mailing addresses were compromised. However, Target was validated as being PCI-compliant two months before the breach. Heartland Payment Systems also admitted to a breach in 2009 that affected as many as 94 million credit card accounts, despite its PCI-compliance.

Today, the continued frequency and severity of breaches have resulted in far more substantial fines. However, regulatory compliance still serves as the bar of accountability, even though it is no longer valid with modern computing methods. These requirements need to be retooled, as national standards are not a bad idea for making sure companies are on the same page. This would greatly assist small- and medium-sized businesses that cannot afford to manage the security investment Solomon conundrum.

Standards need to breathe with emerging threats, modern computing methods and business trends. One of the biggest issues with current regulations is the periodic nature of compliance assertions.

Given companies are often found to be non-compliant during a breach, compliance standards should evolve to require continuous validation requirements. The security industry's support tactics also need to evolve in tandem and require more authoritative validation of cyber-hygiene. Make the adversary work harder, while you work smarter, and balance realistic budgets with maximum security

Chris Kennedy

CISO and VP of Customer Success, AttackIQ

Chris has more than 20 years of cybersecurity risk and operations practitioner experience. Previously, he led the development of the U.S. Department of Treasury's and the U.S. Marine Corps' Cybersecurity Operations Programs.

@AttackIQ

ARE CISOS THE NEW SALES EXPERTS?

Has the CISO role evolved from a tech-laden one to a discipline of effective language, sales and marketing skills? *Sarah Coble* finds out

The chief information security officer (CISO) has traditionally been a technical whizz who can achieve compliance, protect data and clean up when security disasters strike.

Historically, the role has reported to the chief information officer (CIO), but with more CISOs than ever running a direct line to the board or CEO, has the role morphed into a business-focused sales position in which security is sold as a 'product' to the C-suite and the wider stakeholders?

The CISO role owes its existence to a $10m cyber-heist perpetrated in 1994 by Russian hacker Vladimir Levin against the banking giant Citigroup (then Citi Corp. Inc.). To prevent further catastrophes, a team led by former Citi Corp CEO John Reed set up the world's first executive cybersecurity office and hired Steve Katz as the first CISO to run it.

Other organizations followed suit, and today the CISO role is common. A 2018 study by (ISC)^2 revealed that 86% of organizations that consider themselves adequately staffed with cybersecurity talent have a CISO, as do 62% of Fortune 500 companies, according to research published by Bitglass in September 2019.

The Multifaceted CISO 25 Years On

Citi Corp hired Katz to restore trust in the company; to explain what had happened and, through the creation of a robust information security system, to protect the organization from future threats.

The CISO of 2019 has more of a multifarious role, requiring an expansive skillset, and technical focus has given way to business concerns.

"The CISO role has become less of a technical evangelist and subject matter expert and more of an ambassadorial business partner, strategist and marketeer," Domino's Pizza Group PLC CISO Paul Watts tells *Infosecurity*.

James Carder, LogRhythm Lab CISO and vice-president, views the position as even more complex. "Today's modern CISO is more of a business CISO that understands how security ties into the business. In order to be successful, they have to know security, technology, finance, sales and marketing," he argues.

A Tough Sell

Research from Herjavec Group states that cybercrime will cost the world an estimated $6tn in 2021, and according to Optiv's 2019 *State of the CISO* report, "with the rise of the data breach epidemic, and the imposition of comprehensive privacy regulations like the EU's General Data Protection Regulation and the California Consumer Privacy Act, cybersecurity has become a top business risk."

However, a rambunctious cyber-threat landscape, in which 4.1bn records were exposed in data breaches in the first half of 2019 alone (according to RiskBased Security) does not translate into a CISO being hired by every organization.

Furthermore, an organization with the risk maturity and security sensibilities to hire a CISO may not take the next logical step of ring-fencing funds for cybersecurity.

If CISOs are adopting a sales approach to security, then it might be because organizations have lost sight of what information security actually equates to and why it's valuable. In some organizations, security has taken on the character of an optional bolt-on product instead of an essential element of a contemporary functioning business. This detracts from its intrinsic value as a way to maintain trust between an organization and its customers.

In other instances, the value of security has been inverted so completely that it is now seen as an irritating obstruction to progress. "The problem for security is being seen as a cost and/or a barrier to business agility," says former CISO and now CSO at Context Information Security, David Fox.

Occasionally, organizations fail so completely to recognize even the basic risk-reducing advantages of security that they resort to faking it.

"The view that good security can drive business growth and a healthier bottom line has gotten lost. Unfortunately, many organizations are still using the CISO role as a box-checking exercise to claim they take security seriously, when they, in fact, don't," PAS CISO Jason Haward-Grau tells *Infosecurity*.

Winning Hearts and Wallets

Along with a bad reputation in some corners, cybersecurity suffers from being intangible, complicated, technical and, to some extent, unquantifiable.

Carder observes: "Security is not a 'product' that is truly quantitative. It is often measured qualitatively, and boards and executives aren't really a fan of feelings and thoughts without critical, quantitative data to back it up."

However, just as CEOs and boards can sometimes be befuddled by the technical side of security, CISOs can be stymied by the difficulty of trying to communicate security's importance to the business in a way that is relatable.

CEOs that are left unsure of how much bang they will get for a buck invested in security will understandably steer funding towards revenue-generating sales and marketing, or the research and development of new products.

Leaders who skimp on security, whether through operational naivety or reckless abandonment, do so at their peril. As Jason Haward-Grau acknowledges, "if you can't grow sales, marketing and products securely, then that's a problem."

Back to School

Where resources are limited and demands on a budget notable, CISOs are forced to flex their sales muscles to secure funding. "The CISO is ultimately selling insurance and risk mitigation from cybersecurity threats," Code42 CISO Jadee Hanson points out.

> ***"The CISO role has become less of a technical evangelist and subject matter expert and more of an ambassadorial business partner, strategist and marketeer"***

However, to successfully compete for a slice of the budget pie long-term, CISOs must do more than sell; they must communicate and educate.

IBM global security advisor Limor Kessem tells *Infosecurity*: "Strong presentation skills to strategically present projects to the executive team and board members can go a long way in helping CISOs highlight the criticality of security, educate their organization on relevant threats and prepare them for potential attacks.

"By delivering information in a more compelling way, security teams stand to benefit from more adequate

> *"The CISO is ultimately selling insurance and risk mitigation from cybersecurity threats"*

budgeting. More importantly, they can benefit from executive sponsorship and top-down support of the security strategy and governance."

CTO and Pharos Security founder, Douglas Ferguson, envisages CISOs going even further, virtually running a business within a business.

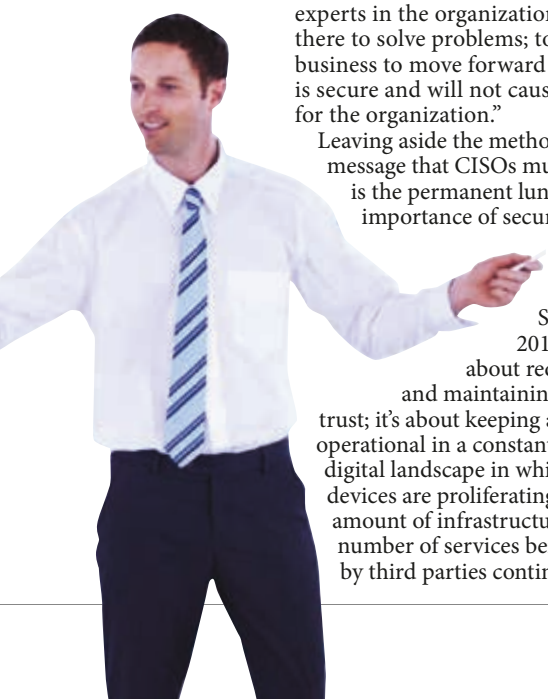
"The successful modern CISO will provide the board with choices, levels of investment that can demonstrably control levels of impact, and the execution plan, down to resource costs, to achieve these results. They will back it up with straightforward and easy to measure KPIs, and provide real-time executive reporting of performance to goal, not only of levels of impact control, but of how well investment is being leveraged."

Get Out Your Compass

The ability to play salesperson, educator or even CEO may now be a requirement of the role, but as an overall descriptor of what a CISO really does, 'enabler' or even 'digital navigator' might be a better fit.

Jadee Hanson says: "If done correctly, security should be thought of as an enabler rather than a 'product.' Security teams should be viewed as trusted experts in the organization that are there to solve problems; to enable the business to move forward in a way that is secure and will not cause undue risks for the organization."

Leaving aside the method, the message that CISOs must convey is the permanent lung-like importance of security to everything a business does. Security in 2019 isn't just about reducing risk and maintaining customers' trust; it's about keeping a business operational in a constantly evolving digital landscape in which IoT devices are proliferating and the amount of infrastructure and number of services being handled by third parties continues to rise.



Simply staying open for business may become increasingly difficult for some organizations, as cyber-attackers switch their sights away from the IT environment towards operational technology (OT).

According to a recent study from Siemens and the Ponemon Institute, "Where past attacks primarily targeted data theft, current and future attacks can hijack control systems and logic controllers that operate critical infrastructure with the intent to cause physical damage and outages."

Bifurcation or Burnout

Whatever the CISO role entails and however it is defined, the job is proving to be too much for many, with burnout becoming a real problem.

> *"The successful modern CISO will provide the board with choices, levels of investment that can demonstrably control levels of impact, and the execution plan, down to resource costs, to achieve these results"*

In a 2019 Nominet survey of 408 CISOs, every single one said their job was stressful, with 91% reporting moderate or high stress and nearly 17% turning to medication or alcohol to deal with the demands of their job. Adding to their worries is the belief held by many CISOs that they are one major security incident away from unemployment.

Cybersecurity recruitment specialist, and founder and CEO of CyberSN, Deidre Diamond tells *Infosecurity* that CISOs "believe their jobs are never secure.

"A phrase I hear all the time is, 'keep your eyes open for me; I could be let go at any time,' and yet they stay committed, hoping it won't happen," says Diamond. "That stress, plus the normal stress of the job, causes complete burnout."

What's Next for CISO Survivors?

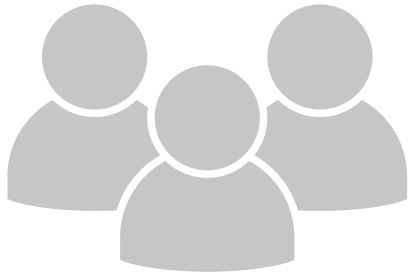
From reactive origins, the CISO now has the chance to be proactive, using a wide range of skills to steer an organization towards a secure and sustainable future.

Bionic Cyber CEO Mark Orlando tells *Infosecurity:* "I believe we'll continue to see CISOs participate in more strategic decision-making and operate outside of infrastructure or information management functions."

As for the future of the CISO role, its first ever holder Steve Katz foresees the position undergoing a long-overdue forking.

In a 2015 interview, Katz predicted: "In the next five to 10 years, the CISO will become two roles – the technology expert and the information risk expert. The information risk role will be the 'what' and the 'why.' The technology role will be the 'how.'

"I think to expect a person to be an expert in both areas will be too much to ask." END



EssentialRETAIL

The Independent Voice in Retail Technology

Delivering What You Need to Know, When You Need to Know it

Webinars

Hear from industry leaders about the latest retail technologies, best practice and hot topics, on demand 24 hours a day

E Newsletters

All the news, reviews and industry developments from the Essential Retail team direct to your inbox – never miss breaking news again

Whitepapers

Download the latest industry research, analysis and case studies from retail technology thought leaders around the globe

Podcast

Listen to the 'Retail Ramble' for a more holistic insight into the retail technology industry from big name brands

SLACK SPACE

Grumbles / Groans / Gossip

01 All-Talking, All-Singing Threats

Walkie talkie toys and karaoke devices hit the headlines for all the wrong reasons in December 2019, as consumer group Which? highlighted potentially hackable vulnerabilities that could be used by strangers to interact with children.

As reported by a number of media outlets, Which? examined various walkie talkie and karaoke devices sold by well-known retailers such as Argos, John Lewis and Amazon. The firm discovered that three out of seven popular toys tested had flaws.

They included the KidiGear walkie talkie made by Vtech, which a stranger could potentially pair with another of the same toy from a distance of up to 200ft away, and the Singing Machine SMK250PP karaoke machine, to which a stranger could possibly stream audio from a distance of up to 10 meters away as the Bluetooth connection did not require authentication.

The findings by Which? are yet more evidence of the safety and security issues that continue to plague connected devices, and particularly highlight risks affecting connected toys used by children.

"The plethora of devices now capable of connecting to the internet or Bluetooth is expanding daily," said Dr Kiri Addison, head of data science overwatch at Mimecast. "These devices often lack even the most basic security measures and are therefore extremely vulnerable to compromise and misuse. This story is concerning as it highlights the vulnerability of children's toys which can be compromised to allow third parties to speak to your children."

Dr Addison urged parents to take an active interest in the range of technology their children are using, as even toys can present an unwanted risk to their safety.

"There are obvious implications in terms of child protection, and current standards internationally are lagging behind in regulating the minimum level of security that should be considered mandatory in the case of any item, which could be considered Internet of Things devices. Children are uniquely vulnerable to influence or coercion via technology and this is something every parent should be conscious of as the sophistication of these often seemingly innocuous connectable devices increases."

02 Baking Security Advice into the Mindset

We've seen missing children photos on cartons of milk, and controversially, warnings about knife crime on boxes of fried chicken. When it comes to cybersecurity warnings though, the French branch of the armed forces with responsibility for internal security has taken an original step, with cybersecurity advice on the paper sleeves of baguettes.

According to French news website *Actu*, for better local communication, the Gendarmerie de la Manche partnered with the action group Cybermalveillance.gouv to distribute 10,000 baguette sleeves which included practical cyber-safety recommendations.

Among the warnings were advice points including: "Beware of beautiful promises," "No hasty clicks," "Do not communicate your personal data," and "Do not give in to blackmail" – all in the French language.

The sleeves were issued after further warnings about account takeover via phishing messages, and scam websites which Colonel Cyril Piat, commander of the provincial gendarmerie group of the Channel, said were prevalent in the "pre-holiday period." He explained that "means of payment, false advertisements are present every year" and the intention of the sleeves was to reach the widest audience with "generic safety recommendations."

This could be an interesting step forward; how many households buy a loaf or stick of bread, and throw away the bag or wrapping? Adding cybersecurity advice to capture one person's attention whilst they are making lunch or waiting for the kettle to boil may prove to be a clever idea.

1. It's not always good to talk when vulnerabilities lurk

2. Making cybersecurity bread and butter?

3. Cryptocurrency cringe!

03 Man Charged After Sharing Cryptocurrency Knowhow

The worlds of cryptocurrency and Blockchain were stirred in November, when a man named Virgil Griffith was charged with violating the International Emergency Economic Powers Act (IEEPA) by traveling to North Korea to deliver a presentation and technical advice on using cryptocurrency and Blockchain technology to evade sanctions.

Griffith was charged with providing "highly technical information to North Korea, knowing that this information could be used to help North Korea launder money and evade sanctions" by the US Department of Justice. It claimed that in his actions, he had "jeopardized the sanctions that both Congress and the President have enacted to place maximum pressure on North Korea's dangerous regime."

In particular, executive orders signed by President Bush in 2008 and President Obama in 2016 prohibit US citizens, organizations and private businesses from lending any aid to the North Korean government. Despite this, and despite receiving warnings not to go, he did so, and attended and presented at the Pyongyang Blockchain and Cryptocurrency Conference.

The DoJ said that Griffith attended in order to discuss how North Korea "could use Blockchain and cryptocurrency technology to launder money and evade sanctions" in a presentation that had been approved by DPRK officials.

After the conference, Griffith is alleged to have formulated plans to facilitate the exchange of cryptocurrency between North and South Korea, despite knowing that assisting with such an exchange would violate sanctions against the DPRK.

Griffith, who is a resident of Singapore, also announced his intention to renounce his US citizenship and began researching how to purchase citizenship from other countries. No stranger to cryptocurrency, he claims to be part of the Ethereum Foundation's Special Projects group.

If found guilty, Griffith risks up to 20 years in prison. Representing him, Brian Klein, partner at Baker Marquart LLP, said that they disputed "the untested allegations in the criminal complaint."

To share your thoughts with us please contact us at ***infosecurity.press@reedexpo.co.uk***

Parting Shots...

Dan Raywood, Deputy Editor

Cast your mind back to the year 2000 – we were in a new world post Y2K, internet was available in homes and Whitney Houston, Faith Hill and Savage Garden were in the charts singing about love.

For me, I had just graduated and was trying to get my first job in journalism, some eight years before getting into cybersecurity. However, one thing cybersecurity-related that did grab my attention in that year was on May 4 when the world was hit by its first major cyber-attack. It was on that date that the ILOVEYOU worm hit users across the globe, and became better known as 'Love Bug' or 'Love Letter.' You could argue that the Windows email worm was not really a cyber-attack at all, but for a few days, there was a lot more love in the room.

It's hard to believe now, but we're close to 20 years since the impact of that worm, and for me it has stood the test of time as a great example of a media frenzy around a cybersecurity incident. It also set a benchmark for how cybersecurity issues would go on to grip the first 20 years of this century.

Love Bug was one of the changing points that shaped current security professionals and procedures. Gavin Millard, now VP of intelligence at Tenable, said that the 1990s involved lots of large virus attacks, but now you see them less, and he put this down to having better inbound defenses on email. "Look at your inbox today, you hopefully don't get spam," he said. "Love Bug was a visual basic script that was emailed to you, and I was an admin when it hit. I knew something was brewing as I saw systems being knocked off in Asia.

"I sent an email to the whole company that said 'If you get an email that says ILOVEYOU delete it as it is a virus' but by about 10am, people were clicking on it and it hit." He later regretted this action, as he said that he could have just put an email filter on to block it.

Mark Sumner was CTO of MessageLabs in 2000. He admitted that at the time, he had seen more complex viruses, but this "sent a lightning bolt" through him as it was pivotal in the fortunes of MessageLabs. Some eight years after the incident, MessageLabs was acquired by Symantec, and Sumner admitted that back in 2000, the company was tiny whilst "externally, we were portraying ourselves as bigger than we were." The company had moved from desktop anti-virus to a cloud-hosted solution, and as this type of virus propagated fast, "the desktop scanner was only as good as the signature." While a small portion of users applied the update, there was a window of six to 10 hours in which people could be hit.

> ***"Love Bug was one of the changing points that shaped current security professionals and procedures"***

Like Millard, Sumner said that he could see something happening as mail queues were building, and the company would run out of capacity in a few hours unless it used more RAID data storage to deal with the growing problem.

The Love Bug – Sumner admitted that on a press call an engineer named it that, whilst others called it Love Letter, hence the multiple names – spread through all addresses in a person's contact list, with the body of the message saying "check attached love letter coming from me." As the file had a long name, the ".exe" was dropped, so the recipient presumed they were looking at a text file.

Its actions were to send the same file to a user's address book, which meant it was successful in spreading. The primary damage came from the impact on mailing systems, and the time and effort spent getting rid of the infection and recovering files from backups. One report claimed that the recovery costs were between $5.5bn and $8.7bn.

So 20 years on, what have we learned from Love Bug? Sumner said that, due to the similar but less impactful Melissa virus, which hit in 1999, some companies were reasonably prepared for something like Love Bug even back in 2000. Since then, the change from Windows to Outlook as the dominant ecosystem means we will not see this type of widespread attack again.

Lotem Finkelstein, threat intelligence group manager for Check Point, said that the success of ILOVEYOU, as one of the very first mass distribution malspam campaigns, paved the way for other threat actors to reach broad audiences. "Since then, hackers improved their techniques and tactics to reach our mailboxes, evading spam filters, and convincing victims to pull the trigger of different infection chains," as well as carefully phrasing messages that look tailored to their recipients and investing in efforts to evade spam filters.

While we may never see something so widespread, and by today's standards so harmless again, Love Bug was a major benchmark for security. It affected businesses around the world, established a need for better preparation and immediate disaster recovery, and hit the media around the world too. Will we see it's like again? Some may say that 2017's WannaCry ransomware had a similar impact, so perhaps it's best to learn from history! END

02-04 JUNE 2020

CELEBRATING 25 YEARS

OF BRINGING TOGETHER THE INFORMATION AND CYBER SECURITY COMMUNITY

infosecurity®

EUROPE

02-04 JUNE 2020 OLYMPIA LONDON

REGISTRATIONS OPENING SOON!

KEEP IN TOUCH WITH EVERYTHING INFOSECURITY

@Infosecurity #infosec20

CLOUDASHUR®

The key to your data™

cloudAshur offers ultimate protection of your data, whether it's stored in the cloud, on your PC/MAC or transferred as an email attachment or file sharing software.

*Amazon Drive, AWS with Amazon WorkDocs Drive, Google Drive, OneDrive, Dropbox/Dropbox Business, iCloud, Box with Box Sync, Egnyte, GSuite with Drive File Stream, HornetDrive, iDrive, Jottacloud/Jottacloud Business, MEGA/MEGA Business, pCloud Drive/pCloud Business, Synx.com/ Sync.com Business, Tresorit/Tresorit Business, Yandex, Microsoft Azure File Storage with the 3rd party software "GoodSync" and many more.

(All listed cloud providers have been tested by iStorage)

www.istorage-uk.com | info@istorage-uk.com | +44 (0) 20 8991 6260

iStorage®