STRATEGY / INSIGHT / TECHNOLOGY

info security

Q3, 2020 / Volume 17 / Issue 3

ADAPTING TO THE 'NEW NORMAL'
How to flourish in IT security's new landscape

MOBILE SECURITY THREATS
Have we reached a tipping point?

FACIAL RECOGNITION
From facts to frictions

FEATURE SLUG

COVER STARS

To celebrate some of the greatest talent in our industry and to visually represent the 'new way of working' addressed in our cover story (p12) and our Zoom feature (p8), Eleanor Dallaway invited some of cybersecurity's brightest stars to appear on our front cover

We asked our cover stars to answer this question: What is the most important thing you have learned during lockdown?

Jenny Radcliffe, aka the people hacker, Human Factor Security
"I've learned that local knowledge is key to survival during lockdown, just as it is key to successful security infiltration. Appreciate your community and know where to find resources!"

Chris Wysopal, CTO and co-founder, Veracode
"During lockdown I have learned that being an optimist is very important in times of change. Recognizing opportunities and being positive to those around you will lead to good outcomes."

Dug Song, co-founder and general manager, Duo Security at Cisco
"To find joy and meaning in serving others in their time of need. We've led in this moment from our hearts versus our heads, and it has made all the difference."

Wendy Nather, head of advisory CISOs, Duo Security at Cisco
"I have learned that Twitter and I need to go to couples' counselling. I've been running my first GoFundMe for someone who is in worse shape due to the pandemic, and I've seen so much love and support come from the Twitter infosec community so I've got to figure out this relationship going forward!"

Kevin Mitnick, the "world's most famous hacker," author and speaker
"I needed to find a way to get from Florida to Las Vegas without flying or staying at hotels, so I purchased a 35-foot motor home and learned to be a bus driver."

Javvad Malik, security awareness advocate, KnowBe4
"I've learned more about my colleagues from video calls, and their backgrounds, than I ever could have otherwise. Also, that I'm way too judgmental of others."

Thom Langford, founder, (TL)2 Security Ltd.
"No matter what managers have said over the years, you don't need to be in the office to be productive. Also, on video calls, clothes from the waist down are optional."

Jack Daniel, co-founder, Security BSides
"The pandemic has clipped my wings, being stuck at home has forced me to learn patience with the one person I've never had patience with before: myself."

Theresa Payton, CEO, Fortalice Solutions
"The most important thing is what I call the three Rs: respect, reflect and reimagine. Respect the situation. Reflect upon blessings in the moment. Reimagine your personal and professional life."

Jeff Moss, founder and creator, Black Hat and DEF CON
"I realize I don't need a lot to be happy, and that I think a lot more about the future of my family and country than I used to."

Graham Cluley, podcaster, Smashing Security
"I wish I could say I learned to play piano, or how to paint, or Cantonese, but the truth is all I learned was how to swear at Google Classroom."

Juliet Okafor, CEO, RevolutionCyber
"The 2020 lockdown taught me to stop trying to be superwoman and allow myself the reality of my flawed humanity."

Rik Ferguson, vice-president security research, Trend Micro
"I learned that I don't require external validation. I do what I do out of a passion for the subject matter and a desire to continue learning and doing that in isolation is perfectly possible. I also learned that I miss the social company of others far more than I thought I would."

Brian Honan, owner, BH Consulting
"I learned that rest and mental wellbeing is critical to ensuring that I can look after my family, my business, my team and our clients. A tired and underperforming leader is of no use to anyone. To support that I learned to meditate, take time out to get some headspace and sleep more."

Talya C. Parker, former global privacy, Converse, Nike
"The most important thing I've learned is how much I value time with family. As a new mother, I was able to witness once in a lifetime milestones with my daughter. I've also learned to cook and enjoy it so much."

Keren Elazari, cybersecurity analyst, author and researcher
"This pandemic has changed the reality of so many people and organizations that depend on us as security professionals, so we have to change ourselves, evolve and adapt to the new normal. It's time for us to RISE UP to the challenge."

Raj Samani, chief scientist, McAfee
"The best thing about lockdown for me has been the silence of the everyday noise I just implicitly accepted. The cars were replaced by birds, so you could say I really enjoyed the tweeting."

Katie Moussouris, founder and CEO, Luta Security
"The most important thing I learned during lockdown is that travel isn't as exhausting as being on video chats for work all day, and that teachers should be paid more than politicians."

Mikko Hypponen, cyber and privacy expert, F-Secure
"My tip for when the next worldwide pandemic hits is this: buy a good webcam, as they will quickly and globally sell out."

Dan Geer, computer security analyst and risk management specialist
"I've learned I like living in a sparse and rural world more than I thought."

James Lyne, CTO, SANS Institute
It seems James is still thinking...

Camille Stewart, cyber and tech attorney, foreign policy specialist, national security professional
"I have relearned I can do anything I put my mind to and that creating space to try new things and focus on me is extremely important to mental clarity and effectiveness."

Professor Sue Black OBE, professor of computer science and technology evangelist
"I learned that I should chill-out a bit more, it's really helped me to focus."

Ed Tucker, CEO, Byte™
"To ensure that I take time to break and switch focus away from work. It is too easy to remain embroiled when what you need is an escape and reset."

Amar Singh, CEO, Cyber Management Alliance
"I've learned I can survive without coffee and Diet Coke and have started exercising daily. I started intermittent fasting (no food, just water) for 20 hours daily and have lost weight!"

Dr Jessica Barker, Co-CEO, Cygenta
"Lockdown has, for me, been a reminder that my time is finite and time is the most precious resource that we all have."

Becky Pinkard, CISO, Aldermore
"Through necessity, I've learned to draw a line between 'WFH' and 'being at home.' I'll never be perfect at it, but I've learned to close the laptop and walk away to focus on my family."

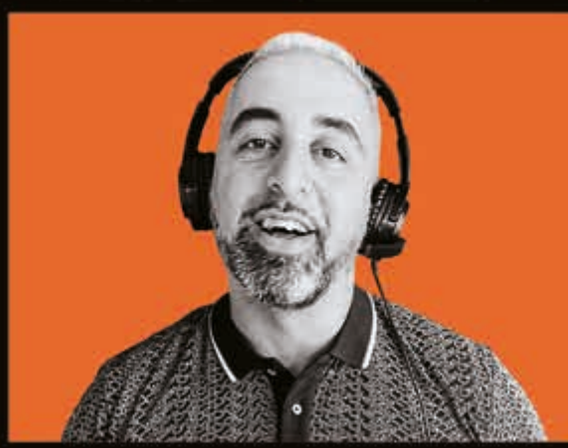
Troy Hunt, founder, HaveIBeenPwned
"I learned to take more time away from the keyboard and invest in my own mental wellbeing."

Clive Room, director, Pulse Conferences
"As a man who lives alone, the main thing I have learned during lockdown is that it's an absolute pleasure to spend so much time with myself!"

Mihoko Matsubara, chief cybersecurity strategist, NTT Corporation
"I have been amazed and pleased by the commitment of many cybersecurity experts and companies to offer free services and form cyber-threat intelligence sharing alliances to tackle cyber-attacks during the pandemic."

CONTENTS

ADAPTING TO THE 'NEW NORMAL'



As companies look to adapt to long-term remote working norms, *James Coker* explores what new and innovative cybersecurity practices we can expect organizations to adopt in the coming months and years

The COVID-19 crisis looks set to change society permanently in a number of ways, one being a huge expansion of home working across all sectors. As the pandemic struck earlier this year, organizations around the world were forced to act quickly to continue operating outside the confines of their corporate offices.

For the many companies unprepared for remote working, at least on such a scale, this has necessitated the rapid deployment of technologies, ranging from video communication software to VPN solutions. Brian Honan, CEO of BH Consulting, comments: "COVID-19 has forced the hand of businesses to adopt remote working and cloud services, and to make their businesses much more digitally agile than they had planned."

With the genie now out of the bottle and the benefits of remote working – such as greater flexibility for employees and reduced overhead costs for companies – being increasingly recognized, there is unlikely to be a return to the pre-COVID world of business. Whilst this new flexibility and utilization of technology is to be welcomed, the speed at which it has occurred has caused a significant headache from a cybersecurity perspective. Manoj Bhatt, head of cybersecurity and advisory at Telstra Purple, notes: "If you have rapidly deployed tech but haven't put the right security controls in place then that leaves you exposed."

As well as unsecured technologies, the fact that employees are working without easy access to IT personnel exacerbates security problems. For instance, bad habits by workers, such as using home devices to access corporate systems, have been regularly observed throughout the crisis, making businesses more vulnerable to infiltration. Additionally, remote employees are far more likely to fall victim to scam attacks. "We are seeing an uptick in security breaches relating to an environment where user accounts are getting hijacked because their access has been phished, or they've been reusing passwords from an account that's been breached elsewhere," says Honan.

Nevertheless, these major challenges also provide the potential for far-reaching solutions and a unique opportunity to bring about a sea change in cybersecurity attitudes and practices. The concept of 'zero-trust' has long been preached by security experts, and it is likely businesses will now be far more receptive to such overtones as they look to secure their new way of working.

Bhatt comments: "I think we're going to see a real flexible delivery model going forward in most sectors; we're going to see people want to work more from home, and they're able to do so, so that's going to be a real challenge to the status quo. Cybersecurity is going to have to wrap its head around it."

So what kind of new and innovative cybersecurity practices can we expect to be employed on a widespread basis in the coming months and years?

User Awareness Training

The notion that individuals are the first line of defense takes on even more relevance as home working becomes the norm, with employees increasingly reliant on using their own best judgement to keep corporate systems safe. In practice however, currently not enough staff have the knowledge or training to burden such a responsibility. User awareness training therefore has to be pushed to the fore in this new world.

> ***"Companies need to readjust their mindset to a zero-trust model in other ways to ensure that the appropriate people have appropriate access in the appropriate way"***

The starting point is ensuring employees are far more vigilant and security conscious when working alongside various distractions at home. "Effectively, your laptop was in a corporate environment with lots of security. Now your secure laptop is on a network that is inherently insecure," outlines Sarb Sembhi, CTO and CISO. "Getting employees to think about this and to consider the data protection implications of any data that is left lying around or conversations that could be overheard now matters far more."

This means bringing about behaviors such as locking devices every time they are left unattended, and blurring out the background on video calls.

Encouragingly, the importance of greater user awareness appears to be getting more recognized by business leaders. *The ClubCISO Information Security Maturity Report 2020* shows that security awareness and training is one of the top three areas where CISOs have driven measurable improvements in recent months.

Additionally, there are indications that employees are now keener to educate themselves about cybersecurity, rising to the challenge of these greater responsibilities. Bhatt says: "I'm seeing a big trend of people getting interested and looking to upskill themselves around cybersecurity. We are seeing a wave of education that's happening within the industry."

Focusing on Mental Health

Another hope is that, linked to this need to improve employees' cyber-awareness, a bigger emphasis on protecting mental health will emanate from business leaders. Working from home can place extra stress on people, both for those who have families and are juggling a number of other commitments, and for people living alone, suffering from limited human-to-human interactions. This is especially the case in a time of crisis, and makes employees much more likely to be duped by scams such as social engineering when stress and tensions are widely felt.

Additionally, the uncertain economic climate is only going to exacerbate this problem. In the same way that cyber-criminals seized on people's health worries over COVID-19, they will surely continue to play on ongoing economic fears such as job security. "Users are more susceptible to these phishing attacks on corporate laptops than they would have been at other times. They are vulnerable and employers owe a duty of care to be thinking about those things," adds Sembhi.

Keeping the Cloud and Communications Secure

The rapid move to the cloud that many organizations have undertaken in recent months requires a more robust approach to managing access and permissions. "In the rush to get people working remotely, many organizations may now have people on non-corporate devices or even on corporate devices that can no longer be updated and made as secure as they were when they were on the corporate network," states Honan. "Companies

need to readjust their mindset to a zero-trust model in other ways to ensure that the appropriate people have appropriate access in the appropriate way to get information that can all be centrally monitored and managed."

With remote employees increasingly targeted by phishing scams, including via email, investing in technology that protects workers from these kinds of malicious communications has taken on a heightened sense of importance. This is vital for enhancing productivity as well as cybersecurity. Sembhi explains: "Investing in technologies that stop these messages getting to the end user means that they focus their time on actually getting work done and not trying to filter out what's spam and what's not."

It may even be the case that companies shift away from email as the primary form of online communication going forward, moving towards cloud and app-based alternatives for both security and efficiency purposes. Interestingly, a recent survey by the think tank Parliament Street found that over two-fifths of businesses are considering replacing email as their primary communication channel.

The ability to hold meetings remotely has been a crucial aspect of businesses continuing to function during lockdowns; however, for ease, many companies have been using software not suitable for the kinds of confidential discussions that take place in the corporate world on a day-to-day basis. Gemma Moore, director at Cyberis, states: "The rapid growth of collaboration on platforms such as Teams and Zoom gives adversaries a whole new way to target employees who might not be ready for the threat."

Honan outlines steps organizations should take to ensure video meetings are secure, including always having multi-factor authentication (MFA) capacity and, most crucially of all, using end-to-end encryption. He adds: "You are still responsible for the security of your information and for your obligations under GDPR, so you have to ensure that whatever tools you use are secure."

Enabling Safe Working Wherever, Whenever

The security of VPNs has naturally taken on a greater level of significance since the shift to mass remote working. Some businesses have had VPN solutions in place for some time to cater for having a small fraction of their staff working from home, but these are often not configured for the entire company to do so. Conversely, other companies have had to implement new VPN solutions from scratch this year. As the dust settles and many organizations consider more extensive remote working going forward, steps must be taken to ensure VPNs are fully secured.

Honan says: "VPNs are becoming much more of an important entry point to a network so it's important those systems are properly patched and secured, as well as up-to-date and scaled to the appropriate size. Then you have tools in place such as MFA to verify users and their correct locations, with geo-location isolation preventing people logging in from remote locations."

There is also evidence organizations are increasingly looking to software-defined networking in a wide area network (SD-WAN) as a more secure means of enabling remote connections to a network, with this technology enabling IT teams to more easily manage hundreds or thousands of locations and multiple connections. For instance, a study in June by Barracuda Networks showed that SD-WAN is now the cloud security solution of choice for around half of UK businesses; this suggests organizations are thinking more deeply about securing their systems adequately.

Another positive that could emerge from the COVID-19 crisis is the development of strong continuity plans in the event of disaster scenarios – traditionally an issue far down the list of priorities for businesses. The pandemic has highlighted that emergency situations do occur, and are capable of severely disrupting business processes.

In Bhatt's view, this realization should give rise to a much more proactive approach to cybersecurity going forward, with boardrooms and industry leaders increasingly receptive to the suggestions put forward by CISOs to properly anticipate threats. "Boards will recognize the importance of resilience and they'll look at the importance of cybersecurity," he says. "Proactive security and getting ahead of the curve is absolutely key, whereas I think what we've had to do during COVID-19 is very reactive."

Faith in a Zero-Trust Model

Although it may take time, it seems inevitable that as remote working becomes 'the new normal,' a zero-trust approach to security will follow suit; one that keeps all aspects of an organization's operations secure. This includes communication software, network access and arguably most importantly of all, a workforce well versed in best cybersecurity practices and behaviors.

Sembhi believes that the traditional approach of building strong perimeter defenses around the corporate walls is no longer adequate. He notes: "I'm hoping in the next year or so that the technologies we're offering will be de-parameterized so that we can work from anywhere with a perimeter around each of our devices and ourselves. That zero-trust approach is going to be in place no matter where we work or what we do."

There is plenty of retrospective work required to achieve this, with cybersecurity measures far from keeping pace with the rapid roll-out of mass remote working at the moment. Moore adds: "With businesses having re-architected their platforms in record time to support remote working, many will find themselves accelerating down the zero-trust implementation route because this lends itself so well to the flexible remote working paradigm we have been forced to adopt."

The ability to work securely in such a dynamic and agile way is surely the motivation needed to finally herald a zero-trust cybersecurity approach on a widespread basis END