info security

STRATEGY | INSIGHT | TECHNOLOGY

Securing a Galaxy Far, Far Away

Cybersecurity's Final Frontier

Q4, 2022 / Volume 19 / Issue 4

SHIFTING MINDSET
Tackling Mental Health Head On

JOINING THE DOTS
How to Optimize Cyber Threat Intelligence for the Win

BEC IS DEAD
Long Live Cyber-Enabled Financial Fraud

info security
STRATEGY | INSIGHT | TECHNOLOGY

ATTEND OUR EXCLUSIVE 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 CPE credits
- Enjoy a luxury breakfast, on us!

Make sure you get your invite 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/

CONTENTS

The Contributors...

Beth Maundrill

Editor
Beth is the Editor at Infosecurity Magazine. She joined the team in August 2022 and has spent her career dedicated to business-to-business journalism and publishing.
@GunshipGirl

James Coker

Deputy Editor
With his MA in journalism, James has been with Infosecurity Magazine since 2020. He covers breaking news and the latest trends in information security, whilst also analyzing their potential long-term impact.
@ReporterCoker

Kevin Poireault

News Reporter
Kevin joined the team in August 2022 after several years covering cybersecurity and deep tech in France and the UK. He completed his master's degree in journalism from Sciences Po in Rennes.
@kpoireault

James Ingram

Digital Sales Manager
James helps clients achieve their goals by leveraging *Infosecurity*'s marketing and advertising options. Outside of work James has a healthy passion for films, sport and cooking.
@infosecJames

Infosecurity Magazine

Infosecurity Magazine

@Infosecurity Mag

infosecurity

Editor **Beth Maundrill**
Beth.Maundrill@rxglobal.com
+44 7436 050 850

Deputy editor **James Coker**
james.coker@rxglobal.com

News reporter **Kevin Poireault**
Kevin.Poireault@rxglobal.com

Online UK news editor **Phil Muncaster**
phil@pmmediauk.com

Online US news editor **Alessandro Mascellino**
alessandro.mascellino@protonmail.com

Print and online advertising
James Ingram
james.ingram@rxglobal.com
+44 (0)20 89107029

Digital marketing executive
Riyhaad Squire
riyhaad.squire@rxglobal.com

INFOSECURITY GROUP

Marketing executive **Alex Casserley**
alexander.casserley@rxglobal.com

Portfolio director **Saima Poorghobad**
saima.poorghobad@rxglobal.com

Event director **Nicole Mills**
nicole.mills@rxglobal.com

Sales manager **Abiola Agbalaya**
abiola.agbalaya@rxglobal.com
+44 (0)208 9107817

Production manager **Andy Milsom**

To amend or update your print subscription, please log in to your user account here:
https://www.infosecurity-magazine.com/my-account/login/

To cancel your subscription, simply return this magazine to sender to be removed from the mailing list or alternatively complete the short request form here:
https://www.infosecurity-magazine.com/my-account/unsubscribe/

For more information about how we process your data including your rights, please refer to our Privacy Policy:
privacy.rxglobal.com

ISSN 1754-4548

Online Summit

INFOSECURITY MAGAZINE

Now On Demand

Unlock Learnings & Network with the Global Cybersecurity Community

14	11	02
SESSIONS	CPES	DAYS

www.infosecurity-magazine.com/online-summits

Register now to access industry-leading education sessions covering the latest trends and technology in the cybersecurity space, including:

- Tackling the Scourge of Cryptocurrency Thefts
- Achieving Security By Design
- Can IoT Devices Ever Be Secure?
- Latest Trends in Nation-State Cyber-Threats
- Quantum Security – Preparing for the Future

WATCH NOW

EVERYONE AND EVERYTHING YOU NEED TO KNOW IN INFORMATION SECURITY

Infosecurity Europe is the meeting place for the industry's finest minds. Delivering expertise and knowledge from the world's most celebrated cybersecurity experts, connecting practitioners with suppliers to find true solutions, and bringing together industry peers to network, share and ultimately, grow stronger and more resilient together.

Build by RX

Find more information: infosecurityeurope.com

@GunshipGirl

From the Editor...

Taking the reins

This edition of the *Infosecurity* Magazine may be the final of 2022 but, as the title's new editor, it marks my first.

This year the team has seen some changes that you, our avid reader, may have picked up on. With that, I'm delighted to introduce you to myself and our new news reporter, Kevin Poireault, and congratulate James Coker on his promotion to deputy editor.

With our new editorial line-up in place, we are already looking to see what 2023 has in store and you'll be sure to see us at events like the RSA Conference, Infosecurity Europe, BlackHat and more, so if you see the team, please do say hello! In the meantime, reach out on social media as we'd love to hear your thoughts on the latest trends and challenges in the information and cybersecurity world. It is an ever-evolving landscape and hearing from our expert community is how we stay informed.

Before looking too far into the future it would be remiss not to take stock of the year that was 2022.

At the end of September, *Infosecurity* Magazine held its second online summit of the year, which included 14 live sessions, a mix of panel debates, #HowTo sessions and keynote presentations. The topics across the two-day event ranged from addressing the cybersecurity skills gap to how to reassure customers about your security and privacy. Other notable sessions included debates on preparing your organization for quantum security and whether IoT devices can ever be secure.

One thing that stood out to me was that during these sessions COVID-19 was seldom mentioned. Just days before the Online Summit, President Biden made an off-the-cuff remark during a '60 Minutes' interview that the pandemic was over.

After discussing security challenges for two days during the Online Summit, it seems that the impact of COVID-19 on businesses is no longer a top concern; one ought to conclude that businesses have spent the last three years dealing with the remote/hybrid work phenomenon and have now had time to implement or begin implementing at least some of the security tools needed to protect a network that now looks very different than it did in 2019.

Now I'm not saying that the cybersecurity challenges brought on by COVID-19 no longer exist, but the issue has certainly moved on beyond the initial knee-jerk reaction to the pandemic.

A big issue continues to be the threat from nation-state actors, which was covered during our North America Online Summit day, including the heightened threat from Russia due to its ongoing war with Ukraine.

We have not seen a major critical national infrastructure (CNI) attack against a Western nation as some predicted after the beginning of the war in the Spring of 2022, and the conclusion of one panelist during the Online Summit was that Russia has not had the bandwidth to do so. We have, however, seen Russia target Ukraine's government sites and CNI companies like DTEK Group – a private energy conglomerate – as a part of its campaign of war, but we've only seen limited instances when this has overspilled outside of the conflict zone, for example DDoS attacks in Estonia which were said to be of Russian origin.

Other nations have also been using cyber-attacks against their foes, for instance Iran's targeting of Albanian government sites, including its border control system. The attacks came after Tirana cut all diplomatic ties with Iran following a July 15 ransomware attack that took multiple government services offline.

Finally, the global economic uncertainty all nations are facing will spell more challenges for those in the cybersecurity profession. As the demand to make a buck entices people into carrying out malicious activities or become more susceptible to threat actor's manipulation, it will be a testing time for individuals and businesses alike.

While the above has painted rather a gloomy picture, I am confident that our community's continued discussion and sharing of experience we are able to facilitate here at *Infosecurity* Magazine through our written work, digital events and in-person gatherings will go some way to inform, educate and allow both cybersecurity enthusiasts and novices to stay abreast of at least some of what's going on. Most importantly, we hope it will inspire them to make innovative and pioneering leaps in the world of cybersecurity.

I am truly delighted to be heading up the editorial team and am looking forward to ways in which we can enhance the experience for our audience and continue to bring you the most important information about the cybersecurity industry.

With that, I bid adieu to 2022.

Beth Maundrill
Editor

LOCKED SHIELDS:

Against a backdrop of war in Europe, NATO's annual 'Locked Shields' cyber exercise took on extra importance in 2022. *Gerrard Cowan* takes a look at this crisis simulation and how the cybersecurity industry gets involved

Sophisticated cyber-attacks targeting critical sectors affects all sections of society, as demonstrated by the hybrid war taking place between Ukraine and Russia. As a result, a plethora of cybersecurity companies, non-profit organizations and institutions with a keen interest in cyber are now working closely with military experts in cyberspace exercises. The collaboration offers a range of benefits to both sides.

There are numerous cyber-focused exercises and activities with a strong military element. The largest such example is 'Locked Shields,' an annual exercise organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The Tallinn, Estonia-based organization works with the alliance without being a formal part of the NATO command structure.

The 2022 exercise included more than 2000 cyber experts from 32 nations. It was based on a 'red team vs blue team' scenario in which a fictional Atlantic island – Berylia – suffers a coordinated wave of cyber-attacks against its military and civilian IT systems.

The exercise, held in April, featured a heavy military component, including representatives from the Estonia Defence Forces and the country's Ministry of Defence (MoD). However, it also comprised a range of other organizations of varying sizes and focuses within cybersecurity. One such contributor was Hack The Box, a provider of online cybersecurity training solutions.

> ***"These are massive exercises involving maybe hundreds of people"***

According to the firm's CEO Haris Pylarinos, Hack The Box contributes to Locked Shields by creating content, including "some of the challenges presented at the exercise." It has performed similar work for other military exercises, including Greece's Panoptis event, to which the company contributed content for the past two years. Pylarinos is also a former winner of Panoptis.

Such exercises are a unique experience for companies like Hack The Box, says Pylarinos, because the scenarios involved focus on "all of the operational aspects that militaries would include." This is not simply a cyber-attack, he notes, but a cyber-attack that involves physical moving parts, many of which are not

PREPARING FOR CYBER WARFARE

restricted to defense systems but cut across critical national infrastructure and the private sector: for example, communication platforms or power grids.

"They have a lot of tabletop exercises and decision-making on how to respond to the crisis," Pylarinos tells *Infosecurity*. "It's not just about the purely technical side and it's not just hacking something or defending something. It's about how we operate."

Such exercises provide organizations like Hack The Box with insights into the needs of military entities and how they view the potential impact of a cyber-attack. The scope of events like Locked Shields also provides significant benefits, he adds.

"These are massive exercises involving maybe hundreds of people," he says. "The way you organize and operate is much more structured than what you see in a five-person team within an organization."

Merging Military and Financial Services

Another participant in Locked Shields this year was the Financial Services Information Sharing and Analysis Center (FS-ISAC), a non-profit cybersecurity community for financial services that has members in 75 countries. Cameron Dicker, FS-ISAC's director of global business resilience, says that exercises are a key tool in the financial sector's cyber defense toolkit, with FS-ISAC participating in such events and organizing its own.

FS-ISAC has participated in Locked Shields for the past two events and plans to do so again in 2023. It coordinates and oversees the exercise's financial sector scenarios, in terms of designing the scenarios and collective response. Its membership's experience is leveraged to design the financial systems used and the cyber-attacks conducted upon those systems, while it also designs a strategic track for senior decision makers, in which they must grapple with societal unrest, interdependencies and misinformation campaigns.

Speaking to *Infosecurity,* Dicker highlights the tight interconnections between the financial domain, the military sector and other critical security and economic priorities.

"As we have seen this year, a military conflict between two countries can still have a global impact on the cyber-threat landscape, including on the financial sector. This is why such exercises are a key tool in global cyber defense," he says. While FS-ISAC runs many sector-specific exercises, "the world is complex and messy, with all sorts of interdependencies. The cross-border, cross-sector nature of cyber threats means we need cross-border, cross-sector, public-private defense capabilities, which is what we are building with exercises like Locked Shields."

Diversity of thought and experience is nearly always beneficial when it comes to cyber resilience, Dicker adds. Cybersecurity teams that have the same background and experience view the cyber-threat landscape in the same way; they are more likely to miss things that would be caught by someone with a different perspective.

"The same situation exists across sectors. Cyber-resilience grows effectively through sharing insights and experience between entities with differing experiences, threat landscapes and strategies. This is especially true of learning from the public sector, which is extremely mature when it comes to intelligence collection and utilization, as well as defense strategies and capabilities."

Some of the biggest names in tech have been involved with such exercises, including Microsoft, which took part in Locked Shields 2022. A spokesperson for the company says that with the growing importance of

cloud environments globally, such exercises "provide NATO nations and our partners with critical experience using the latest tools and capabilities to protect and defend vital cloud-based

sectors come to the table with their own ways of talking about an impactful cyber event.

"In some cases, we are using the same words to talk about different concepts,"

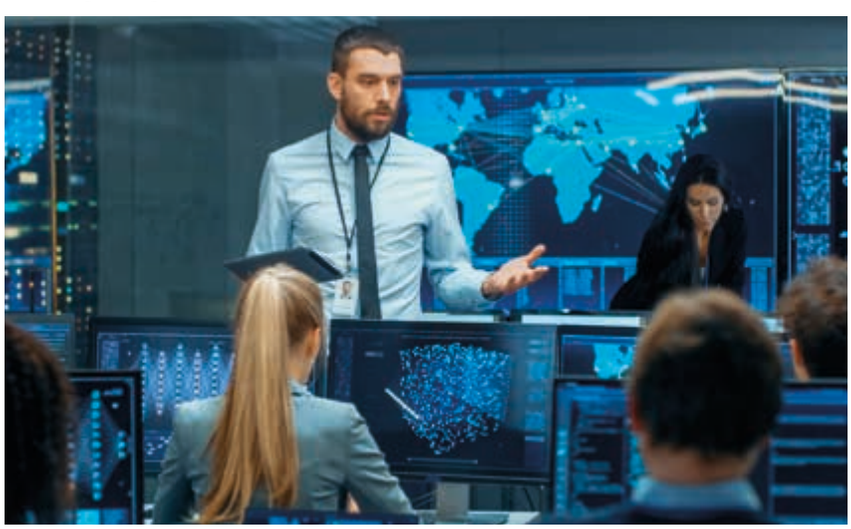
> ***"The cross-border, cross-sector nature of cyber threats means we need cross-border, cross-sector, public-private defense capabilities"***

IT resources from growing nation-state threats." The company is involved with a range of other programs around the world that involve national defense organizations, the spokesperson adds.

One of the challenges of participating in large-scale exercises like Locked Shields is often an issue of lexicon, says Dicker: participants from different

he comments. "However, this is part of the reason we participate in these kinds of events. We do not want to be guessing at terminology in the middle of a crisis response."

FS-ISAC plans to continue participating in such exercises, Dicker says, while it is also developing a new series of exercises for the financial



sector that will test the sector's crisis response procedures in a more hands-on fashion.

"Both the public and private sectors can learn from each other's strategies and defense tactics," he argues. "Understanding how the private sector responds to cyber threats gives the public sector a fuller picture of the impact on society of cyber threats and how they can best deploy their resources to protect citizens."

IT Across the Domains

Finnish cybersecurity provider Arctic Security has contributed its software solutions and a range of other consultancy and training expertise to Locked Shields. Jarkko Huttunen, the company's head of solutions, believes the exercise brings a unique scale and intensity.

Additionally, Huttunen said the exercise brings a level of flexibility in terms of private-military and government cooperation, which "makes it appealing for private companies to participate, as opposed to purely military exercises."

Huttunen emphasizes the degree of overlap across sectors when it comes to cyber, including the military. "IT is IT in both [military and civil] domains, and defending them is something that involves both the military domain and civilian infrastructure."

For Pylarinos, the collaboration between a range of experts from different domains offers clear benefits.

"The more people you involve, the more insight you gain. That's something that any organization – either public or private – will benefit from."

This year's Locked Shields exercise acknowledges the potentially devastating impact of cyber-attacks of critical infrastructure, and the need for a coordinated response across the public and private sector. Amid an increasingly uncertain geopolitical landscape, such preparations are essential END

Q&A

ADENIKE COSGROVE

It's fair to say Adenike Cosgrove is a people person. She has a deep understanding of the 'human factor' in cybersecurity, such as the psychology behind social engineering techniques used by threat actors and how to properly engage people in awareness training.

By James Coker

What's your proudest achievement (can be professional or personal)?

Speaking first-hand to a room of clinicians, nurses and other healthcare workers at a major private healthcare organization in the UK. It was the first time they'd ever really had contact with a security professional to understand the threats they were facing and what to do. We know from our research that these frontline staff are often the most targeted by cyber-criminals, who realize that they are rushed off their feet and more focused on treating patients than checking whether an email is spoofed. The nurses had no idea that they were top of the list due to the access they have to patient data. They now view themselves as defenders not just of patient care but also of patient data.

What was your route into cybersecurity?

Although I really wanted to be an artist as a kid, I was told I could be one of three things: a doctor, an accountant (my dad's preference – he was an accountant) or an engineer. So, being a Daddy's girl but still wanting to rebel, I picked engineer. I've then worked my way through various fascinating roles as an analyst at Canalys and Forrester, developing a deep understanding of the challenges CISOs face and developing cybersecurity strategies for countless organizations.

What one piece of advice would you give to someone starting out in the information security industry in today?

My advice to anyone who wants to pursue a career in IT is to find their grit and go for it without being intimidated by the obstacles they might encounter. This is what it always comes back to.
Whether you're at the very start of your job search, or have an established IT career, my advice remains the same: Get your name out there. Constantly put your hand up to attend workshops, technical sessions, networking events and industry shows. Don't be put off by job postings because they sound too technical – there's always the opportunity to learn on the job, and remember, IT teams require diversity and a plethora of skills.

Quick-fire Q&A

If you weren't an infosec professional, what would be your DREAM job? (And you can't say anything IT Security related!)
An artist.

If you could create an 'all-star' project team to work with you on a really tough but exciting project, who would you pick and why?
I couldn't pick an individual – there is some amazing talent out there. For me, it's more about working with experts that help to fill gaps in expertise.

Who do you really admire in the industry?
Anybody who is helping in the fight against cybercrime is a superstar in my eyes!

What's your guilty secret?
The fact that my husband *thinks* I want to move out to the country and get a dog, when really, I'm a city girl through and through!

BIO

@nikecosgrove

Adenike (Nikki) Cosgrove is VP, cybersecurity strategist for EMEA at Proofpoint, where she drives marketing strategy across EMEA markets. She provides expertise on key regional cybersecurity strategies such as people-centric security, risk management, data privacy and compliance. She works closely with global brands to understand the threats they are facing and feeds that back to the product development teams on help in the fight against today's sophisticated threat landscape.

SECU
a Ga
Far, Fa
CYBERSECURI

Space systems and services already play a critical role in day-to-day life. *James Coker* examines what it will take to secure the space arena now and into the future

RING
laxy
r Away...
TY'S FINAL FRONTIER

For many people, space conjures up images of fantasy and adventure, providing a wealth of fictional content, from *The Hitchhiker's Guide to the Galaxy* to *Star Wars*. Space provokes plenty of imagination and entertainment but can feel remote and inconsequential to everyday lives.

The reality couldn't be more different. The modern world is hugely reliant on the space industry in areas like communication, navigation, timing and weather monitoring. Frank Schubert, head of cyber programmes Germany at Airbus Defence and Space tells *Infosecurity*: "Over the last 50 years, satellites as well as space systems and services have evolved to become a fundamental pillar for nations across the globe touching economies, sustainability, energy, civil protection and many aspects of a citizen's daily life."

This has made this industry a tempting target for cyber-threat actors, who have the potential to impact critical services, whether for financial gain or to damage geopolitical rivals. For example, the Russia-Ukraine conflict provides a stark reminder of how cyber-attacks on space assets can be weaponized by nation-states.

is not fanciful to suggest that over the coming decade and beyond products may be manufactured in space and space tourism could take off; we could perhaps even see the colonization of other planets.

This promises huge benefits, but also greater and potentially terrifying consequences from cyber-attacks. Jenai Marinkovic, executive director, CISO, advisory board - GRC for Intelligent Ecosystems Foundation, believes that cyber-attacks in space will pose a threat to life as well as systems and data. "As an example, I could take control of the flight control systems on a ship that has tourists or consumers on it and hold it for ransom."

It is crucial that the particular cyber challenges for the space industry are understood and acted upon before this dystopian scenario becomes a reality.

The Unique Space Frontier

One fundamental problem posed by growing activity in space is the lack of established rules regarding appropriate behaviors as there is on Earth, according to Marinkovic. "There's no definition for what is permissible in space, what a space norm is," she explains. "If it's allowed in space then there's not much that can be done."

> ***"Following the Ukraine-Russia war, satellite communication providers faced cyber-attacks and disruption to their services"***

Todd Moore, vice president of encryption solutions at Thales, notes: "Following the Ukraine-Russia war, satellite communication providers faced cyber-attacks and disruption to their services. Also, a recent cyber-attack targeted ViaSat satellite modems that prevented customers from connecting to the Internet, while SpaceX's Starlink terminals were jammed in a separate incident."

The cybersecurity challenge is only going to exacerbate. Looking ahead, the sky's (or more accurately, the space's) the limit for the space industry. With the cost of rocket-launch decreasing, this arena in no longer solely the preserve of nation-states or intergovernmental organizations like NASA, as highlighted by enterprises by entrepreneurs like Elon Musk and Richard Branson. It

She anticipates that without such rules, heavy competition between commercial entities and nation-states could spill into cyber-attacks being used routinely to damage rivals and steal intellectual property. Currently, the rules in space are governed by the Outer Space Treaty 1967 which was composed at a time when only two nations – the Soviet Union and the US – had spacefaring capabilities. This treaty offers very limited guidance on what is permissible in space, and certainly not in respect of cyber.

Given significant global tensions and the high levels of competition between private companies in space, Marinkovic predicts it will be a "slow slog" before a comprehensive set of rules are agreed. "I think we're going to see some severe incidents to catalyse why we all need to work together."

Another issue is the growing interoperability of the systems used, creating more connections from Earth to space. This is removing the "technology barrier" for cyber-threat actors, says Daniel Fischer, head of the applications and robotics data systems section, European Space Agency (ESA). "If you are able to hack a system on the ground, you are able to hack the same system in space if you have the right access channel," he notes.

Thales' Moore concurs, highlighting how the commercialization of satellites has led to increased connectivity and familiar systems being utilized. "A few years ago, satellite systems were static as there was no software onboard and the ground control segment was controlled singularly – shut off and disconnected from the internet. Since then, some parts of the system have been replaced with community software to implement new capabilities such as improved telecommunication, navigation and crypto agility. In short, there are now multiple actors who have access to the satellites and those who operate them, including the software and programmable elements; this creates a greater attack surface for malicious actors."

The problem is exacerbated by the fact that many space assets are in service for long periods, up to two decades in some cases. Fischer notes that "you cannot exchange pieces of the spacecraft when it's up," meaning many of these assets are vulnerable to attacks enabled by technological advances. A particularly pertinent example of this is quantum computing, which experts believe will be capable of breaking existing encryption methods in the next 5-10 years. Fischer says that the ESA is investing heavily in post-quantum cryptographic systems to be able to place them on spacecraft as soon as possible to mitigate this risk. "We know it's coming and we have to plan for it," he states.

Increasing Collaboration

It is clear that greater collaboration and agreement is required to mitigate the substantial cyber-risks in the space sector, especially given the distinct lack of international rules currently governing this domain. While political agreements look a remote prospect at this stage, cybersecurity standards for organizations operating in space are more realistic. This includes in areas such as threat intelligence sharing, and minimum security standards for the technologies in use. "International

standards will provide reliable sets of cybersecurity requirements depending on the needs of specific missions: ranging from science missions over commercial to military applications," says Airbus' Schubert.

> *"You are going to have to respond at lightning speed"*

Encouragingly, a number of initiatives are taking place to achieve just that. International standardization groups such as the Consultative Committee for Space Data Systems (CCSDS) and the European Cooperation for Space Standardization (ECSS) are working on developing standards in areas like supply chain management. In 2020, the US government published a policy directive, Cybersecurity Principles for Space Systems, which outlined five main principles for space system owners and operators to follow.

These are positive steps but require all stakeholders to be engaged with time to be effective, from governments to private satellite operators and software providers. "Industry will need to be invested and involved in such activities to ensure they anticipate and reflect changes in their products," says Schubert.

Tech Solutions

It is also clear that significant investment and advances in emerging technologies are required to overcome the unique cybersecurity challenges in space. One emerging area is quantum-secure cryptography and how to ensure such solutions are in place before 'Q Day' — the date when quantum computers are able to break existing cryptography.

Additionally, AI technologies need to be taken to another level to help secure space systems, says Marinkovic, with intrusion prevention systems needing to interact with physical systems. She is also concerned that "there's not a lot of knowledge on how to properly secure an algorithm," and this must be a priority when it comes to the use of AI and automation in space, where there will be more reliance on such systems.

At the ESA, Fischer explains that there is significant work ongoing in the area of optical communications – essentially using light to carry the signal – to secure data flows to and within space. The agency is also developing a specific R&D cybersecurity track, which requires approval from all member states at its Council of Ministers meeting in November 2022. If agreed, "there will be a lot of investment and activities in areas like AI, optical communication, zero trust architecture, post-quantum cryptography systems and secure spacelink technology," he says.

The Human Factor

It is also vital to recognize that securing space is not just a technological challenge, but a human one. Marinkovic believes the skillsets required by cybersecurity professionals will exceed those required back on Earth for a variety of reasons. "We're going to have to be more skilled in the hard sciences, in physics, thermodynamics and mechanical engineering to understand how digital systems work with physical systems," she observes.

Cybersecurity professionals in the space domain are also likely to undergo stress and hardship beyond the high levels already experienced in the industry. This is partly because some personnel may be required to actually live in space for periods. "There's going to be times when you cannot communicate with Earth from lunar systems, and you'll be reliant on human beings on board," she notes. "We currently do not truly understand the levels of stress that this will place on these workers, who will potentially be putting their own lives in danger through their work."

Another aspect is the added pressure brought from the potential life and death consequences of cyber-attacks in space. "You are going to have to respond at lightning speed under immense amounts stress to protect yourself and everybody else who's on that ship with you," comments Marinkovic.

ESA's Fischer agrees that cybersecurity workers in space "requires a special mindset." He points out that in space, it will be even more critical that security measures do not encumber spacecraft operators in their work. "The operator wants as little in its way for saving a spacecraft if it starts tumbling for example," states Fischer. This requires good communication and new ways of thinking to be able to cater for the unique needs of space.

In light of these significant human considerations, Marinkovic believes that "our workforce has to become more technical and think outside of the box in a way we haven't had to do before." This requires a fundamentally different approach to training and recruitment.

She argues that the approaches used in sports training, such as American football, to respond rapidly to events in a game, are applicable for cybersecurity professionals in this domain. "In sports, we have the mindset of detecting and responding rapidly and they drill like that – that is the type of behavior you're going to have to execute when in space."

Marinkovic also believes that neurodivergent individuals could be best suited to certain cybersecurity roles in space, especially those required to physically go into space. "People who are neurodivergent are comfortable with being by themselves, following processes and thinking outside the box," she notes. Therefore, relevant organizations must update their recruitment strategies to identify and entice such individuals.

Reasons for Optimism

There are a number of unique challenges to overcome to secure the space industry, both now and in the future. As space travel itself has highlighted, we should never underestimate the ingenuity and adaptability of the human race in the face of adversity. Fischer believes that cybersecurity in space will evolve through experiences over time. "I'm not overly concerned because all the other industries have gone through this," he observes.

There are people already thinking and planning ahead for securing space in the future as mankind expands its reach into the final frontier END

BETH MAUNDRILL, JAMES COKER AND KEVIN POIREAULT

INFOSECURITY MAGAZINE

IntoSecurity

PODCAST

EVERYTHING YOU NEED TO KNOW
ABOUT THE LATEST CYBERSECURITY HEADLINES

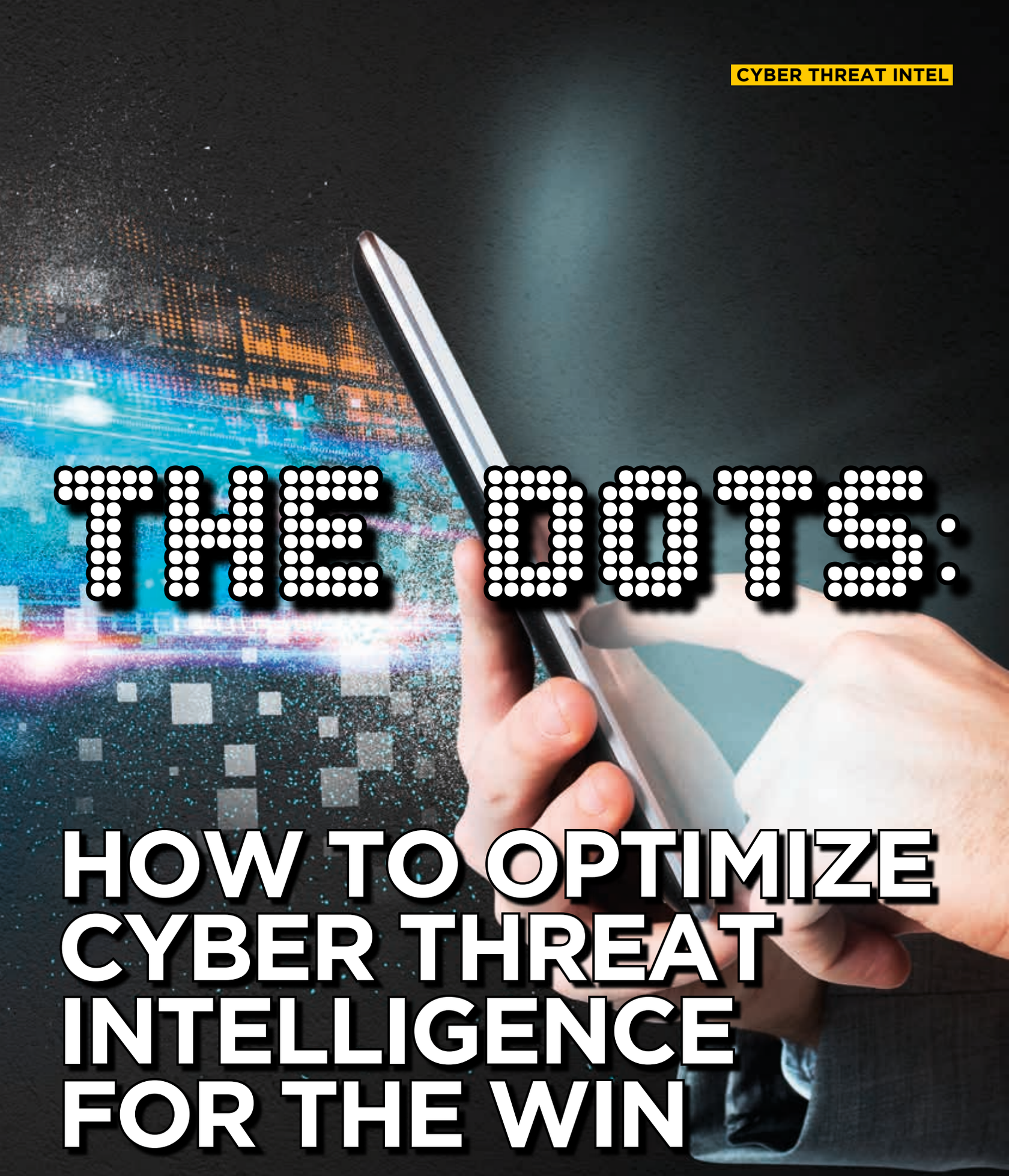
LISTEN NOW - AVAILABLE ON ALL MAJOR PODCAST PLATFORM

SCAN ME
TO LISTEN

WWW.INFOSECURITY-MAGAZINE.COM/


y
MS
PODCASTS


VOTING



THE DOTS:

HOW TO OPTIMIZE CYBER THREAT INTELLIGENCE FOR THE WIN

Phil Muncaster investigates what can be done to consolidate and deliver the information network defenders need

Cybersecurity has always been a strategic business enabler. The difference today is that in a post-pandemic world, where organizations are struggling to wrest competitive advantage and battling continued business uncertainty, even the C-suite gets it. An August 2022 PwC study compiled from interviews with over 700 US execs found cyber ranked as the number one business risk – higher than talent acquisition, inflation and rising production costs.

An effective cyber-threat intelligence strategy could be the difference between managing this risk successfully and letting malicious adversaries retain the upper hand. But even organizations well supplied with internal data feeds may struggle to obtain the detailed and contextualized external threat information they need to make faster, better informed security decisions. This is a challenge that spans industries and regions. Fixing it will require a similarly expansive and inclusive approach.

The Value of Threat Intelligence

There is emerging a concerning imbalance between network defenders and attackers. On the one hand, security teams are understaffed. The global shortfall of professionals is estimated at 3.4 million, according to (ISC)²'s *2022 Global Workforce study*. They're also struggling particularly inside the security operations center (SOC), where a myriad of siloed point solutions sap productivity, create visibility gaps and spit out an overwhelming volume of alerts. Research confirms that 70% of SOC teams are suffering emotionally as a result.

This comes amidst a flurry of spending on digital transformation both during and after the COVID-19 pandemic. It may have been necessary to support hybrid working, enhance business processes and create new customer experiences, but it's also expanded the corporate attack surface. Over two-fifths of global firms believe this environment is "spiraling out of control." With newly published CVEs on track to hit another all-time high in 2022, it's easy to see why.

On the other side, threat actors continue to innovate. The ransomware as a service (RaaS) model is thriving, earning participants billions of dollars annually. Fraud is also peaking on the back of stolen data, with 2021 another record year for scammers in the US. Plus, as threats from both cybercrime and nation-state actors' worlds continue to merge, emboldened state actors are broadening their sights. It's bad news for consumers, companies and governments.

Yet threat intelligence offers a rare opportunity to level the playing field with an agile, determined and increasingly well-resourced adversary. Whether it's strategic, tactical or operational intel, it promises to unlock greater understanding of threat actor motives, targets and behaviors, with which to drive a more proactive security strategy. In this way, it could help everyone from senior executives as they make high-level strategic decisions to SOC teams looking to prioritize alerts. And fraud teams looking to alert customers with early warning of data theft, to operational teams who want to prioritize CVEs for patching.

The strategic importance of threat intelligence is such that President Biden's Executive Order in May 2021 includes a lengthy mandate designed to remove information sharing barriers between contracting IT/OT service providers and the federal government.

Collaboration Considerations

Best practice threat intelligence should involve gathering and processing data from a wide variety of sources. These could range from government bodies to non-profits, academia, industry vendors and sector-specific bodies like Information Sharing Analysis Centers (ISACs). The data they hold might vary a great deal – from high-level white papers and presentations to more technical details like attacker tactics, techniques and procedures (TTPs) and indicators of compromise (IOCs).

Mandiant senior threat intelligence advisor, Jamie Collier, tells *Infosecurity* that governments have been stepping up in this space over recent years, with efforts led by the UK's National Cyber Security Centre (NCSC) and the US Cybersecurity and Infrastructure Security Agency (CISA).

"We are also seeing more public-private initiatives that combine the different perspectives held across government and industry. However, regardless of the initiative, it is vital that they remain focused on intelligence sharing rather than information sharing," he adds.

"Sharing raw and unprocessed threat information puts a lot of the heavy lifting and analysis burden on recipients. Intelligence sharing, by contrast, necessitates sharing far more actionable and easy-to-consume insight. Sharing intelligence rather than information can therefore help to improve security outcomes in a much more tangible and direct way."

Some mature industries like financial services have pioneered industry collaboration between peers, he argues. However, there are persistent commercial and legal concerns which can become stubborn barriers to progress.

"Unfortunately, sharing intelligence can be looked upon as sharing vulnerabilities or weaknesses, rather than helping others to protect themselves from the same type of cyber-attack. These sensitivities are often reinforced by legal and regulatory factors. The only way to break down this barrier is to build trusted relationships, but that is easier said than done," Accenture Security cyber investigation, forensics & response lead, Mark Raeburn, tells *Infosecurity*.

"Taxonomies and nomenclature can also present a huge problem for organizations. Of course, there are obvious benefits to using your own nomenclature for tracking different groups/cyber-threat actors, as it allows you to categorize things in a manner consistent with your own observations rather than those of third parties whose aperture and perspectives may be different. However, this results in a lack of industry-wide consistency, with many organizations feeling like they have to operate and maintain some kind of Rosetta stone."

This is where adherence to industry-wide standards like STIX and TAXII

> ***"Sharing raw and unprocessed threat information puts a lot of the heavy lifting and analysis burden on recipients"***

can help. However, it's not only external barriers that organizations must break down to enhance threat intelligence, but also internal ones, Forrester principal analyst Brian Wrozek tells *Infosecurity*.

"Beyond the vast array of technical challenges that are well known, organizational structures and politics hinder collaboration and data sharing," he argues. "Information is power and people are reluctant to relinquish it. Departments that control information and systems may have competing goals that take priority over threat intelligence sharing, or they may have budget constraints."

From the Inside Out

In order to tackle these organizational challenges, firms need to embark on cultural change to drive a unified data-centric strategy, Wrozek continues.

"Foster collaboration to reduce friction. Identify key requirement use cases to drive data integration solutions and justify new technology investments. Highlight the consequences of the status quo such as incidents that could have been avoided or higher than necessary mitigation costs," he explains.

"Also, incorporate strong security and privacy controls into the roadmap to protect all this information. Stay focused on the goals you are trying to achieve with your threat intelligence program. Remember that some use cases can be solved even if the data remains siloed by analysts who can manually connect the dots."

> ***"Information is power and people are reluctant to relinquish it"***

This internal focus can be key, agrees Mandiant's Collier: "Most intelligence analysts are highly focused on the external threat landscape, yet sometimes neglect putting in the time to understand their own organization. Ultimately, it doesn't matter how much an analyst knows about the latest cyber-espionage operation if they are unable to connect with the stakeholders in their organizations, understand their challenges and work with them to identify how threat intelligence can make their lives easier."

"Intelligence teams might be hardwired into disseminating their expertise to various stakeholders, yet high-performing functions should also be spending a lot of time listening too."

However, ultimately the value of threat intelligence comes from its heterogeneity.

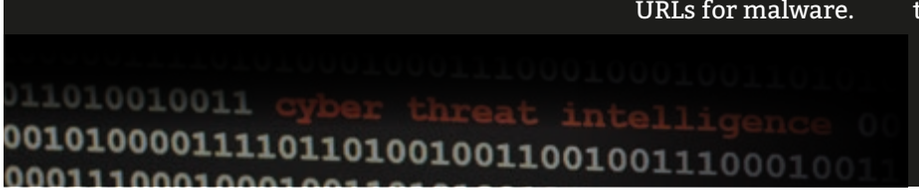
"Different organizations will inevitably have different visibility. This means that there is never going to be one entity that has the best insight. It is instead helpful to see the threat landscape as an area where public and private sector organizations simply have different lenses and perspectives," Collier concludes.

"Rather than seeing this through silos, security leaders will derive more benefit from building up a strategy of collaborating with organizations which offer complementary and useful perspectives. Forming a collective view of intelligence therefore entails a substantive discussion on the unique perspectives of different parties." END

Five of the best independent threat intel sources

The market for threat intelligence is crowded with competing vendors, some of which offer a free version of their services. However, CISOs will want to complement these with some truly vendor-neutral sources. Here's an example of some of the most highly regarded, to feed into threat intelligence programs:

1. **ISACs:** Sector-specific hubs for critical infrastructure owners and operators.
2. **FBI InfraGuard** Free feeds are categorized by industry and joining provides an opportunity to access more localized intelligence.
3. **VirusTotal** A service which should need no explaining. Aggregates AV and scanning engines to analyze user-submitted files and URLs for malware.
4. **Automated Indicator Sharing (AIS)** A CISA service designed to enable participants to exchange machine-readable cyber threat indicators and defensive measures in real time.
5. **Cyber Security Information Sharing Partnership (CISP)** A joint industry-government service set up by the NCSC which allows UK organizations to share cyber-threat information in a secure and confidential environment.



TOP TEN

Fines Issued for Data Protection Violations

01
Didi Global – $1.2bn

In July 2022, China's cybersecurity regulator, the Cyberspace Administration of China (CAC), fined global mobility technology platform Didi Global a record 8.026 billion yuan ($1.2bn) for violating the country's network security law, data security law and personal information protection law. Two Didi executives were separately fined 1 million yuan each for the infringements. The company said it accepted the CAC's decision.

02
Amazon – $877m

The biggest fine issued under the GDPR to date came in July 2021 when Luxembourg fined tech giant Amazon €746m ($877m) for non-compliance with general data processing principles. Amazon has since appealed the decision, which will be heard at a Luxembourg court in January 2024.

03
Meta/Instagram – $402.2m

Ireland's Data Protection Commission issued a massive €405m ($402.2m) penalty against social media site Instagram following an investigation into its handling of children's data in September 2022. The fine was partially based on the fact Instagram had allowed children to run business accounts, thus exposing the minors' data. Instagram's owner Meta said it intends to appeal the fine.

04
WhatsApp – $267m

Ireland's Data Protection Commission has been behind another of the largest fines in this area, issuing a €225m ($267m) penalty against the popular messaging app, WhatsApp, in September 2021. This was due to the firm failing to discharge GDPR transparency obligations. WhatsApp, which has since amended its privacy policy, has appealed the decision on the grounds that the fine was "entirely disproportionate."

JAMES COKER

Top Ten: Fines Issued for Data Protection Violations

Since the EU's GDPR legislation came into force in 2018, issues around data protection and privacy have come to the fore globally. Growing legislation has given regulators the power to hand out severe punishments for data protection violations, and numerous high-profile companies have been hit hard as a result.

Below are the 10 biggest fines issued for data protection violations at the time of writing. Unsurprisingly, the list is dominated by penalties handed out by European regulators under the GDPR. Interestingly, the biggest fine issued to date came from a Chinese regulator. This list comprises of fines issued by regulators and does not include legal settlements with individual victims.

05
Google – $170m

In December 2021, French data protection regulator, CNIL, fined Google €150m ($170m) for failing to enable YouTube users to refuse cookies as easily as they could accept them, thus benefiting YouTube's targeted advertising model. Fines were split between Google LLC, €90m ($87m), and Google Ireland, €60m ($58m).

06
Uber – $148m

In September 2018, it was announced that Uber had agreed to pay a $148m penalty to all 50 US states and the District of Columbia for allegedly concealing a 2016 data breach in contravention of state data breach notification laws. The settlement also required Uber to adapt its data breach notification and data security practices.

07
Facebook – $68m

France's CNIL again issued a fine relating to failing to obtain proper cookie consent from users, this time against Facebook in January 2022. While accepting cookies on the popular social media site is a case of just clicking 'accept,' rejecting them is much more complex. The financial penalty issued in this instance was €60m ($58m).

08
Google – $56.6m

In January 2019, Google was hit by a fine relating to data protection violations, again issued by the CNIL. The €50m ($48m) penalty was levied for failing to provide enough information to users about its data consent policies and not giving enough control over how their information is used. Google's subsequent appeal was unsuccessful.

09
H&M – $41.3m

A German subsidiary of H&M was dealt a €35m ($34m) fine in October 2020 by the Hamburg Data Protection Authority for excessive use of employee data. This included holding data concerning employees' holidays, family issues, religious beliefs and symptoms of illness and diagnoses.

10
TIM – $31.5m

In January 2020, the Italian data protection regulator Garante fined telecoms firm TIM for numerous breaches of the GDPR including unlawful data processing, a non-compliant aggressive marketing strategy and invalid collection of consents. The company was issued with 20 "corrective measures" to implement.

SPOTLIGHT ON THE GROWING CYBERSECURITY WORKFORCE GAP

The global cybersecurity workforce gap has increased by 26.2% compared to 2021, *James Coker* analyzes the latest findings from (ISC)²

A total of 3.4 million more workers needed to secure assets effectively, according the (ISC)² *2022 Cybersecurity Workforce Study*.

This is despite the global cybersecurity workforce growing to an all-time high of approximately 4.7 million, representing a growth of 464,000 (11%) compared to the 2021 report.

The 2022 figures represent a stark increase in the shortage of cybersecurity professionals, up from 2.7 million in 2021. The research surveyed 11,779 individuals globally responsible for cybersecurity.

Expanding Recruitment

While the significantly increased gap is a big cause for concern, it also indicates that organizations are taking cybersecurity more seriously, says (ISC)²'s CEO Clar Rosso, speaking to Infosecurity.

"While we saw the gap decrease during the height of the pandemic, most countries are far advanced in their post-pandemic recoveries and are continuing with digital transformation of a variety of back-office and public-facing functions. Hiring and workforce expansion has rebounded in a number of sectors post-pandemic as a result, including cybersecurity, delivering both the growth in the active workforce, as well as growth in the unfulfilled demand for cybersecurity practitioners. It is also encouraging, as the gap demonstrates increased awareness from organizations of the value of cybersecurity within their operations."

Nevertheless, the need for extra cybersecurity staffing on top of an existing skills gap is putting organizations at significant risk. A total of 70% of respondents reported a shortage of cybersecurity employees, with more than half arguing that staff deficits put their organization at a 'moderate' or 'extreme' risk of a cyber-attack.

Encouragingly, 72% of respondents expect their cybersecurity staff to increase somewhat or significantly within the next 12 months, which is higher than figures from the past two surveys (53% in 2021 and 41% in 2020). This follows the 11% rise in workers recorded this year. "The fact the workforce grew by 11%, some 464,000 is cause for celebration. Adding nearly half a million people to the active workforce is a significant investment in cyber safety and defense," Rosso tells *Infosecurity*.

Rosso also acknowledges the importance of government and broader industry initiatives to help organizations expand their workforce, particularly the ability to recruit those from non-traditional backgrounds.

"Efforts like our own One Million Certified in Cybersecurity program, offering courseware and the exam for the (ISC)² Certified in Cybersecurity certification for free to a million people globally, and to 100,000 people in the UK, is an opportunity to bring a whole new generation of cybersecurity professionals into the workforce. From recent graduates to career changers and IT professionals looking to bolster their cybersecurity skillset, schemes such as this remove many of the economic, experience and accessibility barriers to entry that have limited growth in the talent pool and the active workforce," she outlines.

Internal Factors

While finding enough qualified talent was cited as the biggest cause for the shortage of cybersecurity staff (43%), the research showed there were numerous other internal factors organizations should work on to address the skills deficit.

These included struggling to keep up with turnover/attrition (33%), not paying a competitive wage (31%), not having the budget (28%), not offering opportunities for growth/promotion for security staff (24%) and not putting enough resources into training non-security IT staff to become security staff (23%).

Unsurprisingly, stress and burnout are a major concern for cybersecurity professionals, with 70% feeling overworked. Culture and working conditions were a factor regarding whether an employee would leave their job and over half would consider switching jobs if they are no longer allowed to work remotely.

While three-quarters of respondents reported both strong job satisfaction and feeling passionate about cybersecurity work, 68% of respondents with low employee ratings indicate workplace culture impacts their effectiveness in responding to security incidents. Additionally, only 28% said their organization actively listens and values the input of all staff.

A significant proportion of organizations appear to be taking steps to address these areas. Close to two-thirds (64%) of respondents said their organization is providing more flexible working conditions (e.g., work from home / work from anywhere), investing in training (64%) and recruiting, hiring and onboarding new staff (62%).

The study also examined diversity, equity and inclusion (DEI) within cybersecurity teams. More than half (55%) of employees believe diversity will increase among their teams within the next two years. However, 30% of female and 18% of non-white employees said they feel discriminated against at work, and only 40% of organizations offer employee DEI training.

Reasons for Optimism

Summing up the report to *Infosecurity*, Rosso emphasizes that there are signs of optimism despite the challenges being experienced.

"We are seeing a positive outlook for greater diversity in the workforce," she says. "Respondents also reported a strong preference for remote working, something that many now enjoy as a by-product of the pandemic workplace shift that has greatly improved job accessibility in cybersecurity and aids efforts to level-up well-paid job opportunities outside of London and the major cities. Together with a strong organization investment in training and professional development, these insights represent encouraging progress for both addressing the gap and retaining the skilled professionals we already have." END

ManageEngine

DECENTRALIZING IT SYSTEMS SECURELY

Infosecurity Magazine spoke to Sridhar Iyengar, managing director at Zoho and ManageEngine Europe, about how to securely decentralize IT systems without compromising user experience

Sridhar Iyengar

Sridhar heads Zoho Corporation for Europe & UK. Having been with Zoho since inception, he has thoroughly enjoyed building enterprise software products and the journey from a bootstrapped startup to a global company. Sridhar enjoys exploring and discussing topics on using technology and culture to run organizations efficiently, sustainably and responsibly in an agile manner.

Organizations today are taking a decentralized approach to IT systems as they have been forced to adopt technologies and adapt to changes at an unprecedented speed and scale.

"The COVID-19 pandemic has forced decades of technology adoption cycles to be crunched into a couple of years. Technologies that were optional a few years ago are now a necessity and the norm, including cloud adoption, artificial intelligence, machine learning, remote collaboration, the list goes on," Iyengar explains.

Decentralization of IT systems helps businesses to keep up with the new employee experience standards. According to ManageEngine's *IT at Work - 2022 Study* in the UK and Ireland, 56% of IT decision makers believe that decentralized IT improves scope for innovation and 48% of these have already successfully decentralized their IT structure.

Hybrid work cultures and decentralized approaches put IT teams at the forefront of the business. Iyengar explains the IT team is now responsible for tasks such as ensuring a good bandwidth for the employees while IT systems and infrastructure are updated and maintained at the same time.

Digital collaboration has increased with people logging in from different parts of the world, opening up network vulnerabilities. This collaboration has also increased data management investments, according to Iyengar. Manage Engine's *Digital Readiness Survey* 2021 found that cloud usage has increased in 84% of UK businesses.

"We know the security risks that are associated with sudden increase in use of technologies that may not have been built to handle it. This brings us to another challenge – compliance," Iyengar says.

Unfortunately, national and international regulations take time to reflect changes organizations are making, argues Iyengar.

"Organizations must take up the challenge to ensure they stay compliant without affecting the ease of work. IT is going to be more self-organizing and transformational than ever, and processes and standards must continuously adapt to the needs of the distributed workforce," Iyengar says. Resources that can help keep up with security standards include the Cyber Essentials UK scheme by NCSC. But Iyengar notes that "even that was recently modified."

IT Democratization

IT democratization compels organizations to unify their IT services across business functions by automating and integrating business workflows while maintaining security.

As organizations embark on IT democratization, they essentially remove the middle-man while the processes remain unsupervised.

"We call this the shadow IT. This, ultimately, leads to an increased threat landscape. It's an improved ease of access after all, and attackers are ready to exploit that. We found that 45% of UK-based companies have seen phishing threats increase, followed by account hijacking (38%) and social media-based attacks (36%)", Iyengar says.

To democratize securely, Iyengar says you must minimize the attack vector.

"Integration of machine learning algorithms and AI in cybersecurity applications can improve real-time threat detection and automated incident response. Organizations must monitor their cloud infrastructure and gain visibility into network and access requests to keep an eye on things," he says.

People are important too and the general workforce should be trained to create a security-first culture. Finally, he advises automating workflows across critical systems and enhance cross-functional capabilities across the workforce.

Iyengar notes that the ultimate goal of every business is a healthy bottom line, and this largely depends on happy customers. "We know you can't have happy customers, without happy employees," he says "Maintaining optimum levels of user experience for a distributed workforce has been one of the biggest challenges for most organizations. Organizations have realized that the future is in being multi-functional."

Finally, Iyengar says: "Organizations have to keep up to be relevant. Complications in the hybrid work scenarios, which is the future of work, range from employee motivation, innovation and interactions, to ensuring security and regulatory compliance. Organizations will have to upgrade policies, procedures, processes and technologies to overcome these challenges to thrive in the future."

Company Bio:

ManageEngine is the enterprise IT management division of Zoho Corporation. Established and emerging enterprises—including 9 of every 10 Fortune 100 organizations—rely on ManageEngine's real-time IT management tools to ensure optimal performance of their IT infrastructure, including networks, servers, applications, endpoints and more. For more information, please visit manageengine.co.uk.

mnge.it/Cyber

Our solutions

Identity and access management
Security information and event management
Endpoint security | Network security | Data security

"It won't happen to me!"

- Famous words of regret

Cybersecurity solutions
for your business.

Safeguard your IT with

ManageEngine

TWO EXPERTS GO HEAD TO HEAD

Point

Are We Moving to a Passwordless Future?

Yes

Andrew Shikiar

Executive Director, FIDO Alliance

Andrew Shikiar brings extensive experience driving awareness and adoption of emerging B2B technologies to his role as executive director and chief marketing officer at the FIDO Alliance – a non-profit industry association focused on eliminating the world's dependence on passwords.

@andrewshikiar

You might think you've heard it all before, right? A passwordless age is the cyber utopia we all yearn for but promises of totally wiping out passwords feels far-fetched and far off. After all, how do you go about unpicking a thread so tightly woven into your daily life?

Eradicating passwords will take time, but recent industry news and progress is showing we can confidently say the future is passwordless – and getting nearer.

Passwords Are (Nearly) Over! But Why Now?

We all know the pandemic accelerated digital transformation across all sectors, bringing many more services online. Consumers have more passwords, spend more time online and are doing more sensitive activities like banking digitally than ever before – so it's unsurprising that cyber-criminals are moving online to the easiest and most lucrative point of attack.

In a gloomy economic climate, the vulnerabilities created by passwords are hitting small businesses hard too. According to Verizon, 81% of company data breaches are caused by poor passwords. Cloud service providers that are underpinning popular apps and online services are also under heavy attack, demonstrating the importance of mitigating the vulnerabilities of passwords. I'd like to share a recent example from two cloud service providers recently targeted by the same phishing attack.

In early August, several employees at Twilio received text messages from a fake IT department, directing them to a fraudulent website that required a password change. The unfortunate result was a successful takeover of some employee credentials, which enabled the hackers to gain access to internal Twilio systems – including some customer data. Dozens of employees at Cloudflare received pretty much the same messages, but the attack was thwarted as Cloudflare had issued employees FIDO security keys that are tied to users and implement origin binding.

These attacks are only growing in frequency. Using unshareable credentials like security keys and biometrics is the only way businesses and consumers can protect themselves from themselves when it comes to cybersecurity.

Passwords simply don't fit in the future (or present) of security.

How the Change is Happening

In the case of businesses, the integration of strong authentication security keys and biometrics – as illustrated by the Cloudflare example – is undoubtedly the way forward for them to quickly bolster systems with more robust, passwordless authentication. The technology exists, and it's easier and more important to implement than ever.

The tipping point for consumers may be the introduction of passkeys. Apple, Google and Microsoft recently publicly committed to support this FIDO-based approach to make password-free sign-ins a reality and to make the web a safer space for all. It leverages the same action we use to unlock our devices every day – like using a PIN, fingerprint or facial recognition – only now, this action will help us sign into websites and apps, without having to remember a password or dealing with SMS codes (both of which are also phishable).

By making FIDO's phishing-resistant security readily available to consumers across all major browsers and operating systems, and removing the need to re-enroll for every account or device, it couldn't be easier for consumers to make the switch. Crucially, as users don't need to enter a password to enroll new devices anymore or for account recovery, service providers can now actually make moves to safely start taking passwords out of the equation entirely.

Meanwhile...

The backing of big tech is a sign of things to come and a strong start, but ultimately the demise of passwords will only be accelerated by service providers making passkeys available to use with their services. The good news is that we won't have long to wait as there are plenty of major providers working to go live with support for passkeys very soon, which in turn should accelerate broader cross-industry utilization.

Rather than idly waiting by for passwordless to happen, there are a few things we can all be doing in the meantime. For starters, let's share our 'path towards passwordless' experiences – good and bad. Twilio's post-attack response and incident report should be commended, as should Cloudflare's. The idea of 'security by obscurity' needs to die – not telling anyone you've suffered a breach or been attacked doesn't make you any more secure. Security by community will be key to our collective success.

The community element also sits at the heart of the passwordless technology making this happen too. While Apple, Google and Microsoft made a major splash with their joint announcement on passkeys, they are just three of the hundreds of organizations involved in the FIDO Alliance who bring perspectives spanning borders and industries, and whose use cases are also being addressed by FIDO's specifications and implementation guidelines.

While it will take some time, a future that is not dependent on passwords is drawing near. Thanks to a combination of lessons learned, sheer industry will and new approaches that will make passwordless authentication easier for consumers to use at scale

Counter-Point

No

Passwords are a crucial pillar of cybersecurity and will continue to be valuable for years to come – but only if strict policies are in place and adhered to.

Fortunately, many organizations recognize the value of a strong password. Identity and access management, i.e., restricted admin rights, password policies and two factor authentication, is considered one of the 10 key components to cybersecurity by the UK's National Cyber Security Centre (NCSC). According to the *Cyber Security Breaches Survey 2022*, published by the UK government, 87% of businesses and 77% of charities are undertaking action in identity and access management – making it the most actioned area of cybersecurity for UK organizations.

> ***"The password shouldn't go anywhere just yet"***

Password policies do not have to be complex, but they should be re-enforced often and well understood across an organization. Some examples of important policies include:

Never Re-Using the Same Password

A unique password for every account/device is critical for ensuring that hackers cannot compromise a whole network through one breached data point. While it may seem hard to keep up with a variety of different credentials, password managers are a safe and secure way to create and store strong passwords.

Make use of passphrases rather than words

Much longer than the traditional password, a passphrase is a sentence-style string of text that is far more difficult to crack. They are also typically easier to remember than a combination of numbers and symbols!

Refresh Passwords Every Six Weeks

Each organization relies on a different time period before refreshing passwords, but around six weeks to 90 days is an appropriate length of time before a user should be prompted to change their logins. It means that if credentials have been stolen, this data is only accurate for a short amount of time.

Use Multi-Factor Authentication

MFA is perfect for adding another layer of security to a corporate VPN by using pins, devices or biometric/voice technology as a way to authenticate logins. Yet while this extra layer is becoming an essential for users accessing areas like online banking, it is not impossible for hackers to bypass.

Regularly Train Staff on Cyber Hygiene and Best Practices

Cybersecurity awareness training helps to keep password security front of mind for all staff within an organization, especially while working remotely. If teams do not understand why password best practice matters, it is unlikely they will embrace the appropriate policies.

Mandate Password Protection on ALL Devices

Particularly for any company encouraging bring your own device (BYOD) strategies, it's critical to mandate the installation of password-protection applications on personal devices. By providing an additional security control in the event of a human failure, it reduces the likelihood of a threat actor pivoting from a personal device into the corporate network and penetrating critical IT infrastructure.

Recognize that Passwords Only go so Far

While the password is a critical element to cybersecurity, it is not the be all and end all for strong enterprise security. Organizations big and small must recognize the value of components like a suite of relevant back-ups, incident response playbooks and regular dark web monitoring to avoid falling victim to a potentially devastating cyber-attack.

Conclusion

For years, passwords have been a reliable solution for protecting assets and devices. Their value is well understood across industry and act as a crucial reminder of the importance of data privacy and security every time a user accesses their accounts. While solutions like biometric technology are gaining traction in this space, the password shouldn't go anywhere just yet. New technologies may well still be hackable and simply open an organization up to more tech stack complexities and new vulnerabilities. If all of these listed policies are adhered to, with password hygiene front of mind for the whole workforce, an organization would be remiss to move away from passwords any time soon END

Lawrence Perret-Hall

Director, CYFOR Secure

Lawrence has worked in the IT industry for the last decade, and under his leadership, the CYFOR Group has tripled in size over the past three years. In addition to having industry qualifications in Project Management & Leadership, Lawrence is deeply knowledgeable in incident response supporting enterprise and SMEs in managing complex cyber incidents, organizing multidisciplinary responses and leading stakeholder engagement.

@cyforsecure

BUSINESS EMAIL COMPROMISE IS DEAD

LONG LIVE CYBER-ENABLED FINANCIAL FRAUD

With a surge in global financial losses due to BEC, this social engineering attack can no longer be exclusively treated as a simple financial incident. *Kevin Poireault* investigates why security teams need to battle financial fraud

Ransomware and other malware incidents dominate the headlines in cybersecurity, yet a far less discussed threat, business email compromise (BEC), causes organizations the most significant financial losses. According to the FBI's Internet Crime Complaint Center (IC3) *2021 Internet Crime Report*, BEC attacks accounted for over $2.4bn worth of business losses in 2021. It's 48-times higher than ransomware and one-third of all cybercrime losses reported to the FBI that year.

BEC, also known as email account compromise (EAC), refers to social engineering attacks that target individuals to trick them into sending critical information, usually financial, via email. Typically, the scammer spoofs corporate or publicly available email accounts of executives or high-level employees related to finance or involved with wire transfer payments, using phishing techniques or other social engineering methods, and then persuades another employee to do such fraudulent transfers. While staff in finance are ideal targets, anyone in the business is susceptible to being compromised.

Moreover, BEC attacks have constantly been growing in the past few years. From $1.29bn in 2018, the BEC global losses jumped to $1.7bn in 2019 and $1.86bn in 2020. The FBI has recorded a 65% surge in monthly losses between July 2019 and December 2021. In the first quarter of 2022, BEC overtook ransomware as the top threat for the first time in security consultancy firm Kroll's quarterly report.

"What makes BEC such an important threat is that it is a concern for everyone, from Google and Facebook to a tiny local football club or even an individual wanting to buy a house. If you're transacting money, you could be the target of a BEC attack," Adenike Cosgrove, VP of cybersecurity strategy at Proofpoint, tells *Infosecurity*. "People are concerned about nation-state threats, ransomware, or cryptocurrency mining attacks, but the reality is that the basics work. In most attacks, threat actors largely rely on the same techniques, from compromised credentials and user-activated malware to data theft from the dark web that is being shared, sold and recycled among cyber-criminals."

Worse Than it Seems

The aforementioned data paints a bleak picture, but many cybersecurity professionals do not believe these statistics paint a full picture of the impact BEC attacks are having today.

The latest increase in BEC attacks "was fueled by the COVID-19 pandemic," says Bharat Mistry, technical director at Trend Micro. "With many people working from home, it makes them easier targets than normal. When you see an email that you are unsure about, if you are in the office, you might ask your work colleague for a second opinion and decide not to respond," he adds.

Josh Yavor, CISO at Tessian, a British security company, is convinced that "all the numbers we see are underreported." Cosgrove agrees: "The IC3 claims some of its statistics are global, but how many companies report to the FBI outside of the US?" she asks. The same goes for cybersecurity vendors, Mistry argues: "We see the view from our telemetry, based on our solutions only. Globally, the figures could be much higher than we see."

The reason BEC attacks are overlooked is twofold: on the one hand, the attackers are not usually outspoken about this type of hack, compared to ransomware attacks, and it makes it difficult for security researchers to deploy any forensics and for threat analysts to give any attribution; on the other hand, the stealthy nature of BEC and the impact on the targets' finances and image mean that they, too, would rather keep quiet about falling victims to it.

"The most well-known hacking groups with fancy names mainly are geopolitically motivated, like hacktivists or nation-sponsored actors, whereas attackers who use BEC usually are from organized crime groups. They won't display their names before they get prosecuted," Yavor says. Also, the threat ecosystem gets increasingly sophisticated, with a quasi-Fordian division of labor. One actor typically crafts an attack, another does the social engineering work, and a third deploys it.

"Nowadays, the lines get blurrier as well. The criminals are increasingly collaborating, and different motives and attacks tend to overlap. What might start as a 'simple' BEC attack can turn into ransomware. These should no longer be treated as different problems," warns Cosgrove.

On the victims' side, companies are also reluctant to disclose that they have been attacked. "First, they can have been targeted months or even years before the threat actors proceed with asking for a fraudulent transaction. Second, they also can realize they have been abused weeks or months later the transaction happened. While ransomware is very much in your face, BEC is by nature stealthy," Mistry explains.

"While the victim of ransomware can say there is nothing they could have done, BEC involves the mistake of one person within the organization," Andrew Hay, CISO of Lares, said at the *Infosecurity* Magazine Online Summit on September 28, 2022. For all these reasons, experts generally agree that BEC attacks are rarely disclosed, and data on them is at least incomplete.

Cyber-Enabled Financial Fraud

Times are changing and slowly the perception of BEC is evolving, a positive for the battle against these types of attack.

"There are some indicators that things are changing," Cosgrove says. "With more comprehensive threat data, a set of security tools improved with machine learning and behavioral analysis, and court cases, we now have a better idea of the BEC landscape than ever."

"Lately, in court cases as well as on Twitter, some people have been starting to call BEC attacks 'cyber-enabled financial fraud,' and I think this new label shows the changes in perception of the problem. It demonstrates that finally, organizations recognize that what was once labeled as just a business problem that the CFO or a legal representative would deal with is now perceived as a security issue and that they need to bring the security team into this."

While they usually require low-level hacking skills, BEC attacks are increasingly ingenious in the actors' approaches to successfully trick someone into making fraudulent transactions. "They first use marketing techniques to identify who is responsible for what in the organization, basically working like a marketing agency," Zaira Pirzada, advisor at Lionfish Tech Advisors, said during the *Infosecurity* Magazine Online Summit in September. Then, they can use various social engineering techniques to impersonate a high-level executive, an attorney or even a supplier to attack the individual identified.

Meanwhile, Yavor explains, "Some use the most basic schemes, using off-the-shelf toolkits, and others are very sophisticated, sometimes fully customizing an experience for a specific target and slowly building trust before attacking, for instance."

Supply Chain Attacks

Another explanation for the rise of BEC is that they are increasingly multi-faceted. On top of phishing, BEC attackers now use other platforms such as SMS ('smishing'), voice ('vishing') and social media to operate and sometimes combine several channels.

"A message sent via InMail, LinkedIn's message service, gets four

times more response than an email," Jake Moore, global cybersecurity advisor at European security vendor ESET claimed at DTX Europe on October 13, 2022.

Along the same lines, the most successful recent BEC attacks are supply chain attacks, where the threat actor uses a weaker link, such as a supplier, a contractor, a maintainer or a minor partner, to get access to a big enterprise's accounts. "There is an ongoing lawsuit in Virginia, where a threat actor is accused of spoofing a supplier and using their credentials to send emails to another organization and ask them to change their bank details. Almost half a million dollars was wired directly to the alleged criminal," Proofpoint's Cosgrove recollects.

With this complexification, BEC threat actors are no longer looking exclusively for financial data but any critical data – personal, organizational, or industrial data – that they can leverage to get money wired to them.

Innovative Training and Fraud Backtracking

CISOs are battling an enormous amount of threat actors attempting to compromise their organizations and individuals within the company. With BEC attacks, cybersecurity leaders must ensure they have the correct tools and training capabilities at hand to try and prevent attackers making financial claims against them.

"Statistically, today, BEC is the number one type of attack organizations need to defend against," Yavor insists. To do so, the CISO's number one piece of advice is to plan the proper training: "Rather than just telling your employees what a phishing email looks like, as we usually see in simulated phishing campaigns, a better way to raise awareness on BEC is to tell them what behaviors will never happen in their organization," he says.

"In my last training session at Tessian, I told my collaborators: 'No one from the leadership team will ever message you over SMS to ask you to buy a gift card,' for instance."

"It is also essential not to forget to put in place robust and reliable business and financial processes to allow for quick fraud backtracking," Laurie Iacono, associate managing director for cyber risk at American consultancy Kroll, tells *Infosecurity*.

DMARC, SPF and DKIM

As for the technical measures that could be implemented to prevent BEC attacks, experts call for authentication tools like multi-factor authentication (MFA) and access controls, as well as essential email security tools such as domain checks, email filtering and alerts. Some email security solutions also utilize machine learning and/or natural language processing (NLP) to detect abnormal behaviors or uncommon language used by a specific sender, "but these tools only work as well as the sample size and the quality of the source material used to train them," warned Hay during the September Online Summit.

More importantly, all security experts insisted on three free, standardized tools available for every organization, which, when combined, can significantly improve email security yet are still rarely implemented. These are:

- Domain-based Message Authentication, Reporting and Conformance (DMARC), an email authentication protocol designed to give email domain owners the ability to protect their domain from spoofing
- Sender Policy Framework (SPF), an email authentication method which, alone, can only detect a forged sender claim, but combined with DMARC, can detect forged sender addresses during the delivery of the email
- DomainKeys Identified Mail (DKIM), another protocol that allows an organization to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify

"With these tools, you can achieve the ultimate goal when it comes to BEC: pushing the attackers to the margins, to personal Gmail accounts, for instance, where they will appear as less legitimate to request access to financial data," highlights Proofpoint's Cosgrove.

Yavor adds, "Whether BEC attacks can decrease in the future will not depend on new technologies, but on whether organizations deploy the ones that exist. Otherwise, BEC losses are going to keep rising."

Clearly the fact that BEC attacks do not grab headlines like ransomware hacks, doesn't mean they aren't a huge threat to organizations today. Shining a light on this threat vector continues to be critical but organizations must also implement the right tools, technology and training in order to overcome this cyber-enabled form of financial fraud END

Staggering numbers

A consistent top threat

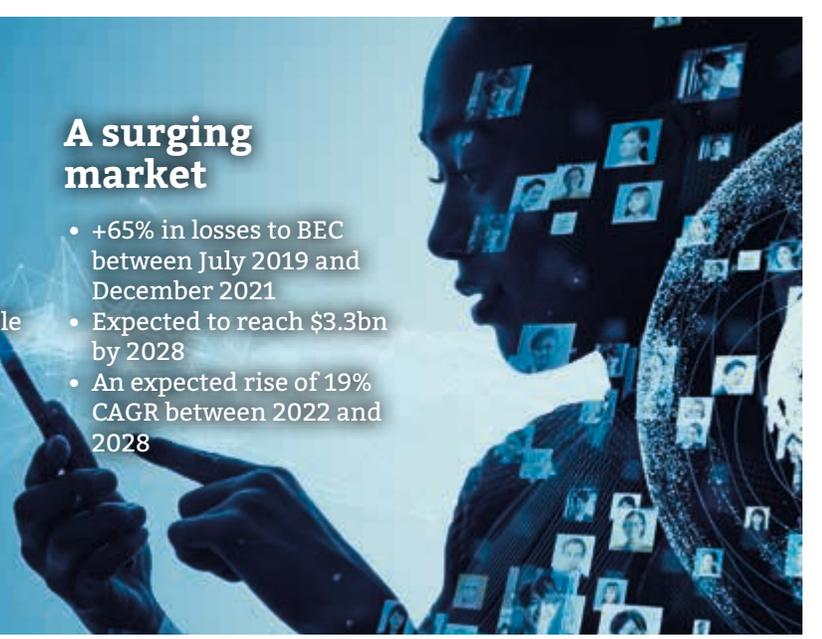
- Top threat in 2022, with 65% of BEC attacks leading to security incidents
- 80% of organizations have experienced BEC attacks in 2022
- Top threat in 2021, with 19,954 BEC complaints reported to the FBI

A lucrative endeavor

- $2.4bn losses to BEC in 2021 (1/3 of all cybercrime losses)
- 48-times more profitable than ransomware
- $43bn losses between 2016 and 2021

A surging market

- +65% in losses to BEC between July 2019 and December 2021
- Expected to reach $3.3bn by 2028
- An expected rise of 19% CAGR between 2022 and 2028



Sources: FBI, Kroll, Osterman Research, ReportLinker

Farms, goats and cybersecurity are rarely heard in the same sentence, but they all apply to the life and career of Jenai Marinkovic. In this interview, *Beth Maundrill* finds out more about Jenai's fascinating life and perspective on cybersecurity

JENAI MARINKOVIC

When you think of a cybersecurity expert, you think Silicon Valley, high-tech campuses, and the bustle of big cities. Not often does your mind wander to a farm in rural California in an ex-gold mining town, surrounded by goats.

"I actually live on a farm and a ranch which I own, and I have hogs and chickens and ducks… and way too many goats," laughs Jenai, kicking off our call by setting the scene in a way I certainly could not have predicted. "I was yelling at my husband this morning; I was like, 'we gotta do something about these goats'!"

Having grown up in a steel mill town in Indiana, Jenai's life journey has taken her through Chicago, New York, Los Angeles, and Silicon Valley before settling into the farming lifestyle in California.

Landing on a farm forced her to look at cybersecurity in a different way, she says. Queue a story about overengineering a solution to prevent deer from mowing down a field of tomatoes.

"My response to the problem was robots. I started building these little Arduino robots because I figured I can just have them go up and down the fields and kind of scan if they see something weird and send me an alert. It wasn't the digital that broke on that, but it was because none of my little robots were ruggedized," she says.

Needless to say, Jenai received some strange looks from neighboring farmers. Plan B was to put up a fence surrounding the tomato field, but that made the entire plot feel like a prison surrounded by huge wire fencing, she explains.

"The long story short of it is I had to rip all of that stuff out and redo it the right way and the right way was for me to sit down, look at who the threat actor was, identify what the asset was that I was trying to protect and then design a security model that facilitates that."

The moral of the story, Jenai says, is that oftentimes in life we don't take a step back and design security from the onset.

"That was a very expensive and silly lesson because at the end of the day what I needed was proper fencing and dogs. I absolutely put tech in places where tech wasn't needed."

Jenai wasn't necessarily destined to work in the cybersecurity field, but had a love for science and technology from an early age; as a child she wanted to be a doctor and then at high school she settled on the idea of being a forensic pathologist.

"It didn't work out that way, so then I went into chemistry and loved it and I also loved biology. For me it was always the hard sciences. Back then it was just a different era, and I didn't know anyone in tech."

Journeys Through Industries

Today, Jenai's curriculum vitae includes time spent at Electronic Arts (EA), in the healthcare industry as an information security manager and as senior director of enterprise security and then IT innovation at DirectTV. Today, she is vCISO at Tiro Security, she is also on the Technology Advisory Board for Beyond a design agency, executive director at GRCIE (GRC for Intelligent Ecosystems), home to the award-winning NextCISO Academy and member of the ISACA Emerging Trends Working Group.

Reflecting on her journey in the biomedical industry she highlighted the switch from working at places like EA and in security consulting to ending up in a highly regulated arena like biomedical development.

The big lesson she says she learned in that field, at a time when security system regulation wasn't as established as it is today, is to be equipped with the correct vocabulary to communicate security and risk without spreading fear.

"I learned a couple of things. One was another way of communicating; it was the first time I understood security and production lines. The way that you design security for that is very different. The other thing is that we were just on the verge, in 2003/2004, of systems being interconnected in ways that people didn't understand. That was the era of 'worms' that move rapidly through these environments, and the way that you handled the block and tackle in those environments is different. But most importantly, the way you communicate must be in line with that company's culture. This was a hard lesson to learn."

This was the launch-pad for Jenai to consider how to build defense frameworks, something that she developed further during her time at DirectTV.

Circling back to the idea of language, Jenai said working for many different companies has taught her that learning how they speak enables you to establish a bond quickly.

"There was one moment where someone else was in a strategy meeting; she had come from large companies and then started talking. I'm not exaggerating, I almost started crying because she was using words that no one else used but that I did use. We were there for hours talking, and it's almost like when you're in a different country and you find someone who is from not just the same country but the same neighborhood and immediately there's a bond."

Leading in Leadership

Jenai has spent a fair amount of time in leadership roles at various organizations. When entering the biomedical industry, it was the first time she was able to establish her own team and work with some really impressive people.

"It was the first opportunity I had to bring people outside of the

world of security into our industry," she says. "Where I really started to learn management skills was when I went into insurance and biomedical manufacturing with Zenith Insurance Company. I had moved into the director role so that the movement from frontline management into middle management was hard."

The difficulty came with the move from managing people to managing managers, who themselves are leaders. The way you do that is very different, and when you are a director, it is a much more political role where you have to manage strategy, operations and budgets.

"That is important, and the reason is there's a lot of people that move into management and leadership positions and security, but they don't manage the budget and until you manage the budget and an operations capability (either security or the newly burgeoning field of regulatory operations) you will struggle to be an effective CISO. Working in insurance gave me that opportunity," she explains.

"One of the big things also was it was the first time I got to do converged security – physical security, digital security and crisis management," she explains. "I was able to manage a guard force across 18 facilities, got to work and design a crisis response plan: the physical security plans as well as digital. There, I really got the chance to say 'well if I'm managing a true security capability then how do these things all integrate? How do they fully operate?' I got to experience that at Zenith insurance."

Another key lesson was in the art of delegation, and the tendency not to delegate when you reach director level, saying she used to believe she could just do tasks faster herself, something many of us in leadership roles have thought on numerous occasions. Jenai reflects on something a mentor had once told her: "You're better off having someone fail 13 times and finally getting it and then doing it right than you doing it and robbing from them an opportunity for them to learn."

When she moved on to DirectTV she said she learned how to hone in on how to use the superpower of failure and remove some of the shame that comes with it. This enabled her to understand that the only way you grow is through failure.

Building at Scale and Designing Security

Her journey into DirectTV came as she was "looking for something a little bit different" and after a successful conversation or two, she moved from the medical sphere to media and entertainment.

Joining DirectTV allowed Jenai to work on building a fully-formed cybersecurity capability from the ground up.

"I was super excited because it meant I could collaboratively build something at scale. I'm always looking towards this future vision of what we can build and the team we can put together to do it," Jenai comments.

Fast-forwarding to the end-result, during her time at DirectTV Jenai was able to build a full-scale cybersecurity capability that extended across IT systems as well as engineering.

"We really got the chance… from governance, risk, and compliance all the way through building a real impressive forensics capability… to build something that was really, truly special, not in terms of just the security, but the team as well," Jenai reflects. "We were all speaking the same language."

> ***"We were all speaking the same language"***

She also notes how TV and media evaluated risk in a very different way to other industries she had been a part of. "Not only that, but we were at the precipice of transitioning from on-prem into cloud at the time. So being in a media entertainment company where they are always pushing the limit when it comes to technology, it was great to be on the forefront especially on those teams."

One interesting element of the organization at DirectTV was that the security function reported into strategy and innovation, Jenai highlights.

"At first, I did not get that. Fortunately, our leadership were pretty amazing and so we were able to do tons of things we needed but I didn't get why security was in the strategy, innovation and architecture department. And with the architecture side it was business, application, data and infrastructure architecture. In all of my previous organizations I'd never seen that before."

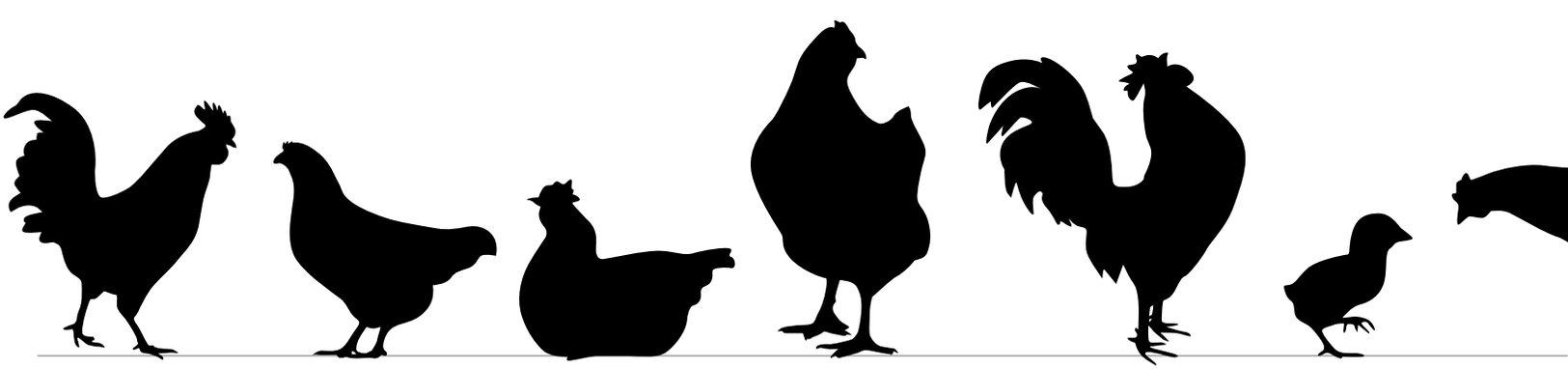
"That was one of the greatest learnings I took into my career – that being embedded for eight and a half years in an architecture, strategy and innovation function meant that security got designed in at the front end of everything at the innovation level," she explains.

Towards the latter years of her time at DirectTV, while she was the head of security, she also had the opportunity to lead the innovation function arm of IT.

She notes that one problem many in the cybersecurity sector still face today is that it is not viewed as a holistic system.

"We look at it as a disparate set of things," Jenai notes. "If you were to architect a human body, I would design an immune system, not just a bunch of separate pieces of highly specialized white blood cells. [Security] is a part of everything - we are a system. The tough part is that security takes time, and everything moves at the speed of light, or now the speed of life."

The pace at which things change puts high pressure on security professionals and Jenai notes how "there aren't enough of us," reflecting on the shortage of cybersecurity professionals the sector today faces. This is something that she has a passion for addressing



in her work with ISACA and GRC for Intelligent Ecosystems (GRCIE).

Digital ecosystems keep growing, but there is a finite amount of security people, she adds.

Passion for People

The cybersecurity skills shortage is a constant in the industry and Jenai notes "there is a lot of talk." However, there are some organizations and initiatives that are attempting to solve the problem, especially in the US at the federal government level.

"The tough part is that you're talking about human transformation," she says. "It's like taking me and saying 'hey Jenai, tomorrow you're going to be working on transmissions for big rigs.' I'd have to completely rewire my brain."

Jenai believes that a lack of empathy within the cybersecurity industry exists and one way to improve the situation is through diversified lived experiences.

ISACA's *State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations* report highlighted the bottom two soft skills valued in the cybersecurity industry as empathy (13%) and honesty (16%).

"When you go through this transformation you have to look at the emotional state of the human involved," she says. Jenai points out that during the six to seven months it takes to get an individual ready for a role in cybersecurity, every single insecurity an individual has will rise to the surface.

"In training, if you don't have a way to help people through that, if you don't have a way to be able to then take that learning that they had and immediately reapply it in their work and so forth, then it leads to people quitting and not being able to get jobs."

Without empathy the jobs are just about technology and the reality is that it is a lot bigger than that.

One way you build empathy is through diverse lived experiences and Jenai notes that only 11% of the cybersecurity industry is under 34 and only 25% of the industry has people of color in management positions.

"I think the fact that we lack diversity in this industry is why we lack empathy and it actually hurts us because attackers weaponize empathy, they don't judge, they understand the emotional state of the person they are targeting and lean into that," she says. "What do we do with our users is we blame them and we scare them."

I ask her what her advice would be, through her lived experience as a woman of color in the industry, to those with a similar background perhaps cautious of making the move into the sector or upwards within the industry.

"Now. Is. The. Time," Jenai exclaims. "Do not squander the light that is being placed on the diversity problems across all areas of tech. Because of that, there are a lot of groups and structures in place to help women, veterans, people of color, and people who are socio-economically disadvantaged get into the world of cybersecurity. This just wasn't there at all when I was coming up."

> ***"Do not squander the light that is being place on the fact that we have diversity problems across all areas of tech"***

The only way to change the statistics that may look troublesome is to jump in, she says. "The first person through a brick wall always gets a bloody nose. There's a lot of people who took a lot of bloody noses in order for you to get here. So don't squander that opportunity and follow your passion."

With her involvement in GRCIE and their NextCISO Academy, Jenai looks to give back and offer people a leg-up towards getting into cybersecurity.

ISACA's *State of Cybersecurity 2022* study illustrates the need for new people to get involved in cyber, with 62% of all respondents reporting their organization's security teams were understaffed. The report notes that, "With four million cybersecurity jobs open globally, it's critical that we completely transform how we train and upskill our workforce with a special focus on our human skills and mastery of security controls."

The NextCISO Academy, which is tuition-free, started with a question – how to get junior people fit for purpose on day one in a junior cybersecurity or GRC role? The three founders, including Jenai, had a unique set of skills that included people and human resources, security specialties, and recruitment. "We felt that we could get someone who had been working in fast food into a junior cybersecurity position," she says.

The program is now on its second cohort of students and Jenai says that the first cohort was able to secure compensation at new roles of between $85 and $95,000 after being part of the academy. With this, she says that the NextCISO team was able to help people with contract negotiations and provide them with the tools they needed to gain successful employment.

The NextCISO academy decided to focus on training governance, risk, and compliance, with Jenai saying understanding GRC helps you understand the fundamentals of building the ship. Also, in GRC, she says you can get up to speed and into a job faster.

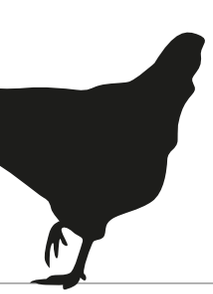
There was also a strong belief that within the training program NextCISO developed, management skills had to start at the beginning of people's careers. Jenai's partner and cofounder, Melissa Elza (a people expert) felt deeply that the time to start training the next CISO is when they first get into the field.

Even in nextCISO's training and apprenticeships Jenai continues to innovate and push the boundaries by integrating virtual reality (VR) and the metaverse into the program.

"Metaverse does a couple of things, it's immersive, there's a haptic response, so there's actually a physical response of what happens to you, and designers can design the learning experience to influence the emotional response of what happens to you when you go into VR. It all helps to imprint on the learner."

In order to see success from your learnings, you must be a strong communicator, and Jenai says that after the metaverse/VR learning and training, students were not as scared to present their work to boards and CISOs compared with if they had taken to the stage without that preparation. The students had been presenting on large virtual stages since the beginning of the class. Its a safe way to become comfortable with presenting content on a stage to a discerning audience.

Jenai is someone who has always been willing to take a chance throughout her career and personal life, enabling her to tell a fascinating story. This also explains her passion for innovation to find solutions to the problems of the modern world, as well as her desire to open the door to a diverse range of people and perspectives. It's a story worth telling, and an inspiring one for anyone looking to forge a career in cybersecurity END



FEATURE

US FEDERAL PRIVACY LEGISLATION: CHALLENGES ON THE HILL

Danny Bradbury investigates the spider-web of state and agency laws that attempt to tackle data privacy in the US and how realistic a federal initiative really is

If information is power, then US data brokers must be among the most powerful organizations of all. They collect and sell information on individuals including their political beliefs, habits, interests and even real-time GPS locations. Much of this happens without the individual data subjects' knowledge.

Privacy advocates would like a federal privacy law to protect this information. Several such laws are in play, but one is gaining significant attention: the American Data Privacy and Protection Act (ADPPA).

Today, those wanting to prosecute privacy-related claims must use a patchwork of laws. Some of these are widely applicable, such as section five of the Federal Trade Commission (FTC) Act, which allows the FTC to sue companies for deceptive practices. If a company mishandles personally identifying information (PII) in violation of its privacy policy, the FTC can make a case that it has misled affected individuals.

This patchwork of laws makes it difficult to prosecute big privacy violation cases. For example, a recent class action suit launched against Oracle in California seeks damages from the company, which is also a data broker and has amassed mounds of data on up to five billion people. The complaint invokes Californian common law and the state constitution, the Unfair Competition law, the California Invasion of Privacy Act and the Federal Wiretap Act. It does not invoke an overarching Federal privacy law because there isn't one.

While Congress continues to equivocate on a federal law, states have taken the matter into their own hands. First, California passed the California Consumer Protection Act (CPPA) in 2018, making it effective in 2020. Virginia and Colorado followed suit in 2021 with their own laws, and this year Connecticut and Utah followed suit. A few other states have privacy bills in committee. There are also dozens of states with data breach notification laws that stop well short of comprehensive data protections.

Then there are industry-specific laws such as the Health Insurance Portability and Accountability Act (HIPAA), which protects healthcare data. Additionally, there are laws protecting specific groups. Consumers can try to hold companies to account under the Children's Online Privacy Protection Act (COPPA), as the government did when it fined YouTube for its handling of children's data.

Federal Accountability

Even now, there are multiple bills in play seeking to introduce accountability for consumer data at a federal level. The International Association of Privacy Professionals (IAPP) publishes a tracker detailing current legislation. The most recent one, published in April, highlighted 17 consumer privacy bills on the Hill in the 117th Congress.

Since then, Rep. Frank Pallone (D-NJ), Chairman of the House Energy & Commerce Committee, introduced the ADDPA. Co-sponsored by two Republican and one Democrat representatives, the bill has bipartisan support. It also received support from Sen. Roger Wicker (R-MS), Ranking Member of the Senate Commerce Committee. Pallone introduced it in June 2022, and it passed the House Energy and Commerce Committee the following month.

> ***"Biometric data and geolocation data, that's where you have a longer list of prohibitions"***

The ADDPA has been well-received by some privacy policy experts. Cobun Zweifel-Keegan, managing Director, Washington, D.C. for IAPP, says that it represents a new way of thinking about consumer privacy protection.

Fair information practices in the US have typically followed a principle called notice and choice, otherwise known as notice and consent. This means notifying consumers about how their information will be used and then letting them make their own choices. However, some think this idea is outmoded and unworkable.

"A lot of recent thinking and scholarship on in the privacy realm has started to raise questions about the utility of that kind of approach and also the ability of consumers to make educated choices, even when a lot of effort is made to educate them."

The relationships between different companies using consumer data and the complexity of what they do with it is beyond many peoples' understanding. Just ask the average customer how many privacy policies they've read.

Instead, the ADPPA takes a more aggressive approach, says Matt Wood, vice president of policy and general counsel at the Free Press Association, which supports the bill.

"There are certain things for which consent is required, but there also is a list of prohibited uses," he says. "So biometric data and geolocation data, that's where you have a longer list of prohibitions."

The ADPPA also includes a civil rights section that prevents organizations from collecting or processing data related to race, color, religion, national origin, sex or disability. It also requires companies to conduct annual impact assessments for algorithms that could cause harm to individuals, reporting on its design, uses, and the data it processes. This would likely affect big tech companies that use AI to manage things like personalized social media news feeds.

There are other provisions in the ADPPA. Like the Europe's General Data Protection Regulation (GDPR) approach, it requires organizations to appoint a privacy officer that will oversee a data privacy program. It also calls for a data security officer.

Other notable measures in the bill include the creation of a registry for third-party collecting entities (which includes data brokers). Individuals will be able to request that all registered data brokers delete all information about them collected indirectly and avoids collecting any more.

The FTC would be instrumental in enforcing this law. The Bill calls for a Bureau of Privacy within the Commission, and a Privacy and Security Victims Relief Fund that will use the proceeds of civil penalties to compensate victims of privacy violations.

The Problem of Pre-emption

The ADDPA has garnered significant attention thanks to its bipartisan support and its fast passage through the committee. However, it is not a law yet, and it begs the question: why has the US taken so long? Congress has been aware of the privacy issue for at least 22 years, since the FTC first asked for a federal privacy law.

"The core issues that are the most fiercely debated and which have been the death blows to previous and current legislation are pre-emption and enforcement," explains Emory Roane, Policy Counsel at privacy advocacy group the Privacy Rights Clearinghouse.

Pre-emption is an especially thorny issue. A law that pre-empts state

legislation effectively replaces it, preventing citizens from using state-level legal measures against violators. As more states pass comprehensive consumer data privacy laws, opposition to pre-emption grows.

In California, opponents are unwilling to relinquish the work already completed on perhaps the strongest state-level consumer privacy law.

> ***"The core issues that are the most fiercely debated and which have been the death blows to previous and current legislation are pre-emption and enforcement"***

"The ADPPA absolutely, unequivocally, objectively would represent an improvement for many Americans in many states that have tried and failed to pass comprehensive privacy laws," says Roane. "That is simply not the case though in California, and arguably it's not the case in other states like Connecticut and Colorado."

Enforcing the Law

The other sticking point in federal privacy legislation is enforcement. State attorney general's can bring civil cases against alleged violators under the ADPPA, but it also allows individuals to bring their own private civil actions.

The provision for private suits, known as the private right of action, only kicks in four years after the ADPPA comes into effect. That doesn't placate Jordan Crenshaw, executive director and policy counsel for chamber technology engagement at the U.S. Chamber of Commerce. He fears a sea of frivolous lawsuits from ambulance-chasing attorneys targeting businesses.

"We're incredibly concerned that private attorneys will have every incentive to throw claims against the wall and see what sticks," he frets.

A carve-out in the ADDPA preserves California Civil Code section 1798.150 from pre-emption. This is the PRA clause that allows consumers to go after violators themselves.

Crenshaw opposes this too. The US Chamber of Commerce will accept nothing less than a law that offers complete pre-emption of state legislation. "It's a new national patchwork, as opposed to really solving the problem of having 50 different state privacy laws throughout the country," he argues.

The Future of ADDPA

In trying to please everyone, the ADDPA's authors have managed to draw ire from both sides. In spite of (or perhaps because of) these political complexities, the bill is an admirable accomplishment, according to Wood.

Wood notes that until this point, nobody else on the federal stage has been able to get Republicans to vote for a bill with a private right of action.

What chance does ADDPA have of becoming law? Privacy advocates should not celebrate just yet. This Congress is tied up in November's mid-term elections, leaving it short on time with a long to-do list. Also, despite its bipartisan support, it faces significant opposition on the Hill.

The Bill may have passed committee, but it still has to get through the House. That requires the support of speaker Nancy Pelosi, who happens to be from California. She opposes the bill based on its pre-emption.

Sen. Maria Cantwell (D. Wa), who has her own privacy bill, the Consumer Online Privacy Rights Act, also opposes the ADDPA on the grounds of enforcement. As chairwoman of the Senate Commerce Committee, she is effectively the Senate's gatekeeper for this bill.

Even if the bill doesn't become law, it could still move the needle forward, says Coburn. "I think this is certainly the main contender for shaping that conversation moving forward, because it's a bipartisan, bicameral bill," he says.

US politics is a strange and inefficient machine. Laws often do not pass, but they spark and elevate conversations. Whether or not the ADDPA makes it to the White House, it will hopefully inch us closer to resolving one of the biggest problems for privacy in the United States and bring more wide-ranging protections for Americans in every state END

How to reassure your customers about your security and privacy frameworks

Mark Nicholls

Head of Information Security, Risk & Compliance, Ramsay Health Care UK

Mark holds overall group responsibility for security management and related governance activities, ensuring that the organisation puts appropriate safeguards in place to protect information assets and business operations. Prior to Ramsay, Mark was CISO at Chime Group, a global marketing, advertising, PR and events company.

@ramsayhealthUK

For the healthcare sector, security and privacy is a top priority.

The data we hold and process is probably some the most sensitive data related to individuals. In fact, there is strict regulatory compliance we must adhere to under the UK's Data Protection Act and GDPR, as health data is defined as special category.

Although primarily an independent healthcare provider, operating 40 hospitals and facilities throughout the UK, we do provide services to the NHS across the country and as such there are data sharing agreements in place. To allow for this, as an organization we must also meet the security and privacy standards laid out in the NHS Digital Data Security and Protection Toolkit – a yearly requirement and published to interested parties.

With this in mind it critically important that our customers are satisfied that we are doing the right thing when it comes to security and privacy in respect of their data, whether they are a private or NHS patient.

We already face an uphill struggle communicating security to our customers, as generally speaking our customers are not interested in security from practitioner point of view, i.e. if one starts a briefing or communication detailing the cryptographic algorithms or complex technical security controls we have in place they will switch off and we lose engagement.

To our customers, security should be somewhat invisible, providing a frictionless user experience. What is important to them is getting the best healthcare services available, while we worry about the security and privacy of their data in the background.

> ***"There will be no technical jargon and the language used will be positive"***

We do this by making sure all interactions are customer focused, while maintaining the balance of security verses usability. We have done a lot of work on the patient journey to underpin our technology choices when it comes to digital transformation. Those choices have resulted in us selecting best of breed security solutions, ensuring our company, staff and patient information assets and the associated technology, applications, systems, infrastructure and processes are adequately protected.

If our choices around security technologies or how we have implemented security into a process results in a negative customer experience, then we have got it wrong!

We want to be open and transparent with our customers around what we are doing with security; as such, we are in the process of developing communications and briefings in a language that we deem "human and kind." This means there will be no technical jargon and the language used will be positive. We will talk about patient journeys and the steps we take in the background to protect data. This will be a combination of high-quality focused security and privacy training for all our staff, implementation of best of breed technical controls and robust processes around security. We will tie this to our public promotion of compliance with standards such as ISO27001 and NHS Digital Data Security and Protection Toolkit, and what this means in jargon free language to those who interact with us.

Our goal is to ensure our approach to security and privacy is customer centric END

Mark Guntrip

Senior Director, Cybersecurity Strategy, Menlo Security

Mark is responsible for articulating the future of threats to security leaders around the world. Prior to joining Menlo Security, Mark has been security strategist at Proofpoint, Symantec, Cisco and several other leading cybersecurity providers.

@menlosecurity

The news has a constant stream of articles about the latest threats and attacks. It seems like every day we are learning about new data breaches and ransomware attacks. It is no secret that the bad guys are working to stay a step ahead of threat prevention solutions. So how can security vendors reassure their customers about their security solutions?

At Menlo Security, we recently conducted a survey that found email was the most cited entry point for ransomware attacks, followed by desktop browsers and mobile devices. Interestingly, evolving threats and remote workers were named as the biggest challenges in ransomware defense. Clearly, phishing is still an effective attack tool. Continuing to educate your teams about the dangers of phishing attacks and how to spot them must remain a priority. But we all know from experience that education and training are not the be all and end all solution.

Ransomware, and most other attacks, are best prevented prior to the initial intrusion. If the threat can be prevented, it means the infection chain never happens. Deploying a security solution that is focused on preventing attacks, rather than detecting and mitigating them after the fact, is the best way to show customers you have a robust security posture. Therefore, demonstrating how your solutions help address pre-attack frameworks (MITRE) as well as the expected attack frameworks (NIST, MITRE), can show a preventative approach to security.

As we see attacks increasing, companies cannot stand still. Security teams need to put a greater emphasis on business continuity and disaster recovery. They should also monitor and respond to the latest threats. Where supply chain attacks have been shown to be incredibly damaging, the risks associated with third-party connectivity and integration should be considered to manage or minimize the attack surface, for example.

> ***"If the threat can be prevented, it means the infection chain never happens"***

As compliance regulations have started to converge with security mandates, there is now a range of certifications that an organization can use to demonstrate its security posture. Everything from ISO 27001 as a building block or organizational security through to more rigorous certifications, such as FedRAMP, and even customer security audits with external validation. Companies that have a wide range of validation with internal and external acceptance can be seen as a secure choice.

Today, users, their data and applications, are all found in the cloud. While all this work is being conducted in the cloud, it is also the one place where traditional security measures – which are still very much relied on – are not located. With web browsers constantly being updated to address vulnerabilities, and SaaS applications further expanding the attack surface, there is more distributed work – and data – to protect.

Securing modern workplaces requires modern security. Coupled with in-depth defense measures, today's preventative security measures involve taking a Zero Trust approach to security that protects productivity where it occurs. Security is most effective when it is applied close to the user, applications and data END

Zaira Pirzada

Advisor, Lionfish Tech Advisors

Zaira Pirzada is a multi-lingual actress, writer, as well as a security and tech advisor with Lionfish Tech Advisors. Prior to joining Lionfish Tech Advisors, she was a security analyst with Gartner, Inc., covering the data loss prevention, file analysis and data masking markets.

@zaira_pirzada

The alphabet soup of security compliance requirements you meet, and the security standards frameworks you certify against or attest to, can get anyone's head spinning, especially your customers.

Ultimately, what they want to know is: "Is my data secure?"

Well, is it? From one audit to another, many security functions piece together their full security and privacy story to convince the auditors that their mix of people, practice and technology yields good security. Most pass the test, sufficing one checkbox after another year after year. This may provide a seal of approval from accredited auditors, but for the customer it is not a true, proper and detailed answer to the question "is my data secure?"

So how do we reassure customers that the sum of our efforts in security and privacy told in our evidence packs to auditors translates to their data being safe?

Here are my Top Three Recommendations:

My first recommendation is that you maintain strong policies, processes and procedures. Your privacy policy should be publicly shared with your customers and detail the following: the different types of customer data you collect; how you collect and use customer data; where you disclose customer data; and the customer's legal rights regarding their data. It would be to your benefit to provide customers with the best email or number to reach your organization to discuss any unresolved questions.

My second recommendation is that you publicly educate your customer via a security-privacy-customer trust page housed somewhere on your website (yes, you need this). Here, briefly explain the importance of your information security management system, privacy function and customer trust. Visitors to this page should know that you exist to ensure the security and continuity of your organization and to build on the relationship of trust between your enterprise and your customer base. On that same page, list the security and privacy compliance certifications, attestations and regulations you abide by.

You should expand on each element of that list with what it is, why you abide by it and how often you are assessed by third-party accredited auditors.

My final recommendation is that you emphasize signing a non-disclosure agreement (NDA) at the initial or renewal contract stage regarding any conversation about the confidential and inner workings of your security and privacy functions. Why? So that the customers who are still not assured by the information you provided in your policies and other publicly facing material can be immediately granted the right to read through your certification and attestation reports, and even dive into your program during a security walkthrough. This is all with the security function's assurance that any information shared will be safe during the length of the customer-provider relationship.

This method is the most time-consuming; however, it is proven to be very beneficial for those larger clients that have deep internal security teams and risk management functions working on answering their detailed, third-party supplier security questionnaires. Though this way is not scalable and should be reserved for the most adamant customers, this truly is walking the talk END

FEATURE

SHIFTING MINDSET: TACKLING ME

'NTAL HEALTH HEAD ON

Stress and burnout are regularly highlighted as issues facing cybersecurity professionals today. *Beth Maundrill* investigates the problems and how mental health is intrinsically linked to the cybersecurity skills shortage

The COVID-19 pandemic spotlighted the stress that cybersecurity professionals experience in their jobs with the drastic move to work from home. Many in the information security sector found that, at home, they were working more hours than ever before, facing new and complex challenges and being hit with a barrage of alerts, requests and security threats.

Nearly three years on, the industry is now acutely aware that cybersecurity professionals can be afflicted by stress, burnout and mental health challenges. Looking at the bigger picture, stress also leads to poor job satisfaction, which sees people abandon their roles in cybersecurity, fueling the skills gap and talent shortage the industry is facing.

"In the cybersecurity world, the 'Great Burnout' has been well underway for quite some time. Although it can sometimes seem unspoken, burnout in the cybersecurity industry is a well-documented issue that is impacting employees everywhere," comments Adam Marrè, CISO of Arctic Wolf.

There are statistics galore surrounding the topic. Email security company Tessian has noted in a report that CISOs on average work 11 more hours than they're contracted to each week, more than half of CISOs (59%) say they struggle to switch off once work is over and shockingly, 44% have missed a doctor's appointment in the last 12 months due to work.

"If you look at a threat map of any company's perimeter security, you will see a constant barrage of incoming attacks. It's scary stuff to watch, especially when you acknowledge the fact that in present times, it is typically not if you are breached, it's when," notes Martin Cannard, VP of product strategy at Netwrix, a California-based IT security software company.

"Is it any wonder then that today's cybersecurity professionals are stressed, waiting for that 3.00am phone call that will potentially kick off days of working around the clock," he says.

Other statistics worth highlighting come from the UK's Chartered Institute of Information Security (CIISec), which polled over 300 industry professionals to compile its *2021/22 State of the Profession* report.

The study revealed that a third (32%) of respondents are kept awake by job stress, and a quarter (25%) by lack of opportunity, but only a fifth (22%) by their organization suffering a cyber-attack.

Amanda Finch, CEO at CIISec, tells *Infosecurity* she finds it "pretty frightening" that so many people were kept awake by job stress.

"[Mental health is] always something that's probably been put to one side in previous years, but we are now more aware of mental health issues and COVID-19 probably brought that forward. It is important that we discuss the issues, address them and understand how people are feeling out there," she says, noting that while mental health is indeed a topic more people are talking about now, the stresses of the job are increasing at the same time.

CIISec's findings show that 12% of people who took the survey were working 50-70 hours a week. Whatever statistics you reference there is a common theme to the issues that people in the sector are facing.

Barriers to career progression were also highlighted, including a lack of confidence in their own ability (38%), lack of support or mentoring (38%), an assumption they lack skills for roles (36%), a feeling of being unwelcome or unaccepted (28%) and a lack of training opportunities (28%).

Arguably, this report found that cybersecurity professionals are more concerned about lack of career opportunities than they are about their organization suffering a cyber-attack.

All of this provides fuel to the fire of the cybersecurity skills gap crisis that the industry is facing. Mental health and retention are intrinsically linked.

One piece of research from Bridgewell Consulting warned that UK critical national infrastructure (CNI) organizations could face an exodus of cybersecurity leaders over the next 12 months due to stress and burnout. The survey of 521 UK cybersecurity decision-makers in communications, utilities, finance, government, transport and aviation found that 95% of respondents are experiencing factors that would make them likely to leave their role in the next 12 months.

All this at a time when it is estimated that 3.4 million more cybersecurity workers are needed to secure assets effectively, according to (ISC)²'s *Cybersecurity Workforce Study* 2022.

> ***"It is important that we discuss the issues and that we address them"***

Taking Action

We are all fully aware of the issues that organizations face when it comes to the health and wellbeing of their staff, including of course cybersecurity professionals, and now is the time to do something about it.

Curtis Simpson, CISO at Armis, comments on how he provides support to his team: "With over 20 years in information security and technology, and more than half of this time being spent in leadership roles, there's one very important lesson that I've learned over the years. It's all about creating a safe space for growth and mentorship."

He says, "Every one-on-one with my team involves listening first and where appropriate, coaching and mentoring on both a tactical and strategic level. Just knowing that there is someone who has been through a situation before and that they will not only help you navigate through the situation if you need the help, but also help you learn from it, alleviates so much of the pain."

As the CIISec report shows, mentorship and career progression are things that many are striving for and not having them is leading to added stress.

Speaking about businesses as an entity, Finch says that they must provide a more supportive structure.

"One of the things that came out of our findings is that the [cybersecurity] industry had been slow to adopt industry standards; where people know what they are doing and what they are working towards really helps a lot," she says.

"I think the management structure within organizations needs to be more supportive. If people are in roles where they feel supported, have the right processes in place and can see where their career paths are going then they are going to be calmer and more relaxed in their environment. Having mechanisms where people can put their hands up and say, 'look I'm struggling' and making it a lot more of a supportive environment."

With this support, Finch points out people are much more likely to stay in their jobs rather than seek alternative roles outside of their current organization.

Ensuring people are in the correct position and "not trying to be a round peg in a square hole" is also vital to employee stress and satisfaction.

"A lot of this is about working with HR department and those departments need to be really cognizant about the problems that are there," she says. "It's not just technical skills that are highly regarded, if you look at the data we have,

communications and analytical skills are in high demand so it's important to upskill people in the softer skills that are not directly the security skills."

Finch notes that ensuring employees are not stressed and have room to develop ultimately links to how security itself is viewed, and its role in the business.

"We're going through something of an evolution, where security's recognized more and more not just as a technical field (i.e. keeping the lights on/keeping the data safe), but as a strategic asset that's intertwined with areas of the business such as finance, risk, compliance and HR – meaning there needs to be more appreciation for the different skills needed, and more opportunity for security personnel with strategic and interpersonal skills to go far."

Be Prepared

For a long time, cybersecurity has been focused on the technology, but we are beginning to see this mindset shift with the understanding that people are at the heart of everything that is achieved.

One way to help people prepare for crisis response in the event of a cyber-attack is the development of cognitive agility.

Bec McKeown, director of human science at Immersive Labs and Chartered Psychologist, tells *Infosecurity* how adaptive problem solving is a key skill for cybersecurity professionals and how cognitive agility can have a positive effect on resilience. She describes cybersecurity as a "wicked problem" where there isn't a clear-cut resolution, meaning people need to be more adaptive in the ways they think.

With the sheer volume of information that cybersecurity professionals can be faced with during a crisis the brain is susceptible to becoming overwhelmed.

> ***"The CISO needs to be able to communicate with the HR department using a language they understand"***

CISOs should be asking whether they are ready to cope when it comes to the next cyber-incident.

McKeown suggests that organizations wishing to embark on this kind of learning and development first conduct exercises in order to find out the current status of the workforce. From there, upskilling can be implemented where needed and leaders can identify what gaps there are in the team.

This is not a one-time thing either, it needs to be reinforced and McKeown notes that these kinds of capabilities can fade if they are not exercised on a regular basis. Exercises cannot be an occasional luxury; regular exercising will enable crisis response teams to make connections between previous decisions and apply them during an incident.

"Being proactive is better than being reactive," McKeown adds.

Being prepared and having the right tools in order to be resilient can be key to relieving some, not necessarily all, of the stress and uncertainty that security professionals face when met with a crisis incident.

CISOs at the Ready

As leaders, CISOs face the pressures outlined in earlier this article but also bare a lot of the responsibility to make sure that their teams are resilient and are not suffering from mental health issues.

"The CISO needs to work with everybody at a higher level," Finch notes. "It's about how you communicate. The CISO needs to be able to communicate with the HR department using a language they understand and hitting their buttons. HR want to have an effective workforce, they want to avoid

[employment] tribunals, they don't want to have large recruitment bills."

McKeown concurred that collaboration is key, and it is important, in general, to have relationships with people who speak a different business language to those in the security realm.

A lot of initiatives, training and resources relating to supporting teams with their mental health and resilience of course cost money. Finch says, "In terms of getting budgets and getting more effective security controls you need to be able to talk to the C-suite about why you need these things, why it's financially good sense to have these things.

"For the CISOs, they need to look inside themselves to see where they need the support to help them to manage their teams. It's taking things out of the security environment and more into the management environment."

Arctic Wolf's Marrè reflects on his management approach when it comes to stress and burnout: "I have made it a priority to set work-life boundaries my entire career, whether it's been at the FBI, Qualtrics or Arctic Wolf. Now as a cybersecurity leader I can use this experience to help my team enjoy satisfying work-life boundaries."

> ***"We're going through something of an evolution, where security's recognized more and more not just as a technical field"***

He adds, "Managing stress and maintaining a workload that challenges, but does not cause burnout, should be a frequent topic in weekly one-on-one meetings and during touchpoints between leaders and team members. Scheduling additional open conversations with teams that center on healthy habits and boundary maintenance can create a positive culture around work-life balance, empowering teams to define their own strategies to deal with the at times crushing workload. Normalizing discussions about mental health in the workplace and removing the stigma around asking for help requires a cultural shift that starts with the C-suite."

It is likely that we will continue to see saddening statistics highlighting mental health issues that cybersecurity professionals face because of their jobs but it is encouraging that today, in 2022, the spotlight is truly being shone on the problem and there are individuals and organizations alike who are tackling it head-on END

Q&A

NICOLA WHITING

Nicola Whiting is an award-winning cybersecurity professional who likes to think outside the box. As someone who is neurodivergent, Nicola is passionate about increasing diversity and inclusion in the sector to enable innovative practices to tackle rapidly-changing cyber-threats. She is also Worcestershire's Commissioner for the UK Cyber Science & Innovation Audit, with significant expertise in the use of AI and automation in cybersecurity.

By James Coker

What's the best thing about your job?

The autonomy I have to try new ideas and the inspiring people I get to work with, both inside and outside Titania. This is especially true of those who are focused on increasing industry diversity, fighting the stagnation of groupthink and increasing innovation and resilience.

And what's the worst?

Finding enough hours in the day and choosing what to work on (too many ideas too little time).

What's your proudest achievement (can be professional or personal)?

My proudest achievement professionally was receiving the Sparky Baird award from the US Military for my news piece on the transition from kinetic to AI-driven cyber warfare. (In military terms it's a bit like being given a Pulitzer and it's a huge honor for a non-US citizen to be awarded it.) Personally, it was taking my husband and our parents to Buckingham Palace to be awarded an MBE for 'Services to International Trade and Diversity' – I think my mum nearly exploded with pride and the pictures of that day are some of my most treasured memories.

Who do you really admire in the industry?

That's a list too long to mention – but people like Dr Jessica Barker, Dr Victoria Baines, Becky Pinkard, Amanda Finch, Sian John, Sarah Armstrong-Smith, Jane Frankland and the many others working to advance both technical excellence and inclusive practices in our industry.

What was your route into cybersecurity?

I was headhunted to help build the business end of a cybersecurity startup and never left!

What's the most misunderstood thing about information security?

That information security is all about preventing access and locking things down. In fact, it's the opposite – it's about giving safe secure *access* to information that people need, when they need it, so they can make successful effective decisions. Information security should enable productivity and provide safe working environments.

Quick-fire Q&A

Tell me in one sentence what your job is about
Building high performing teams that understand their individual strengths and can maximize them to "get things done!"

What's the most important lesson you've learned?
That it's OK for failure to be an option – as long as you learn from it!

Tell me something about you that our readers will be surprised by
I sing on the folk circuit and am known for my Victoria Wood impressions.

What's your guilty secret?
Reading sci-fi and fantasy novels – they're a fantastic way to switch off into pure escapism.

BIO

@CyberGoGiver

Nicola Whiting MBE is co-owner of Titania Group. She is also an Amazon bestselling author, an award-winning leader in the field of cybersecurity and a board member of NeuroCyber CIC (an organization dedicated to increasing NeuroDiversity in cybersecurity).

SLACK SPACE

Grumbles / Groans / Gossip

01 Hacking Starlink Has a Price... and it's Only $25

The war in Ukraine has shown how critical satellite internet can become in times of cyber warfare. For better, when Elon Musk's launch of his Starlink service in the country helped thousands of Ukrainians stay connected. For worse, when the hack of Viasat denied internet access to customers way beyond Ukraine's borders.

It may sound worrying, then, that a single researcher successively hacked a Starlink dish… with a custom toolkit that cost him only around $25.

Lennert Wouters, a security researcher at the Belgian university KU Leuven, revealed on August 12, 2022, at the Black Hat conference in Las Vegas, that he used a fault injection attack to break into locked parts of the Starlink system.

To do so, Wouters stripped down a Starlink dish and created a hacking tool – a custom circuit board known as a modchip, made of a Raspberry Pi microcontroller, flash storage, electronic switches and a voltage regulator – that he attached to the Starlink dish.

The fault injection attack runs the glitch against the first bootloader, which is burned onto the system-on-chip and can't be updated. The attack then deploys patched firmware on later bootloaders, which allows him to take control of the dish.

As Starlink engineers printed "Made on Earth by humans" on their board, Wouters' modchip reads: "Glitched on Earth by humans."

Before going public, the researcher notified Starlink of the flaws through its bug bounty scheme and open-sourced the modchip details on GitHub.

The presentation prompted SpaceX's satellite internet service to publish a six-page response, in which they called the attack "technically impressive."

The company did not deny the researcher's claim that the vulnerabilities are "unfixable" and insisted that they "rely on the design principle of 'least privilege' to constrain the effects in the broader system."

02 Passwords: Paw Patrol is on a Roll

Who would use their pet's name as their password? In the UK, one in 10 people, apparently.

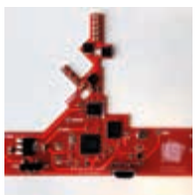
According to a YouGov survey commissioned by the email provider GMX, 10% of British respondents still use the likes of 'Teddy,' 'Bella' or 'Roxy' when asked for a password. Around 7% prefer dates of birth of family members and 3% even use their favorite football club, the study revealed.

However, using personal information for passwords is not an exclusively British issue as 16% of Germans, 13% of French and 12% of Austrians also use loved ones' birth data when signing up to a new service.

Despite relying on beloved pet names, British people actually fare better than their Germanic counterparts when it comes to password privacy: 54% of respondents in the UK said they were not using personal data as their passwords, compared to 48% of Austrians and 43% of Germans passwords.

More generally, GMX found that 46% of us still use personal information for passwords, a serious security risk. A total of 33% of respondents also said they were "hardly worried" or "not worried at all" about being affected by identity theft through stolen passwords – 64% said they were "concerned" or "very concerned."

"Identity theft is a real nightmare for many Internet users. Special attention should be paid to one's email account, because this is how you log into most services and can reset passwords. In addition to a strong, unique password for each service, you should also activate two-factor authentication," said Jan Oetjen, CEO of GMX.



***1.** Glitched on Earth by a single human*

***2.** "Don't do it, Human"*

***3.** Severe consequences*

03 Ex-eBay Execs vs. EcommerceBytes, Feat. a Pig's Head

If you were told that two former eBay executives and five more employees/contractors were accused, and in some cases convicted, of cyber bullying two bloggers, would you believe it? Neither would we.

However, David Harville, ex-director of global resiliency at eBay, and James Baugh, the e-commerce firm's former senior director of safety and security, were sent to prison on September 29, 2022. The former was sentenced to 57 months behind bars, plus two years of supervised release and fined $40,000, and the latter to two years plus two years supervised release and fined $20,000.

They were charged by the US Justice Department with participating in a plan in 2019 to harass and intimidate Ina and David Steiner, who publish the newsletter and website EcommerceBytes. The two bloggers were critical of eBay.

Five other former eBay employees/contractors allegedly took part in the cyberstalking campaign, including Philip Cooke, was sentenced to 18 months behind bars in July 2022, as well as Brian Gilbert, Stephanie Popp, Veronica Zea and Stephanie Stockwell, who are currently awaiting sentencing.

To silence the Steiner's, the seven individuals are alleged to have harassed them online and offline between approximately August 5 and September 6, 2019.

The accusations include sending private Twitter messages and public tweets criticizing the newsletter's content, sending threats to visit their hometown Natick, Massachusetts, to surveil them and install a GPS tracking device on their car, and even posting live insects, the severed head of a fetal pig, a funeral wreath, a pig's head mask and a book about coping with the loss of a spouse to their house.

All the seven accused co-conspirators pleaded guilty.

In their civil complaint, the Steiner's have also named as defendants former executives not charged by the government, including Devin Wenig, former CEO of eBay, Steven Wymer, former SVP and chief communications officer of eBay, security contractor Progressive FORCE Concepts, LLC and eBay itself.

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

Parting Shots...

James Coker, Deputy Editor

We are fast-approaching the end of 2022, which has once again proved to be a highly impactful – and challenging – year for the cybersecurity industry. It is important to take the time to reflect on some of the major events, and to put them into the wider cybersecurity context.

The COVID-19 crisis finally seems to be abating, and this year, life has returned to some form of normality for the majority of people. Nevertheless, security professionals are still getting to grips with legacy of the pandemic, particularly remote working and the acceleration of digital transformation, which has led to an enormous growth in cyber-attacks. The cybersecurity industry is adapting to this new environment by implementing more appropriate tools and technologies for the new threat surface, and crucially, enhancing employee cyber awareness.

The news cycle in 2022 has been dominated by the events of the devastating Russia-Ukraine conflict, which started in February. In addition to the death and destruction caused by bombs and bullets, this war has had a significant cyber dimension, with Russian threat actors frequently attacking Ukrainian government and critical services. These have ranged from low-level DDoS strikes to take down websites to attempts to cripple critical infrastructure services through malware. On the flip side, pro-Ukrainian hackers have targeted Russia in retaliation, including streaming independent coverage of the war on Russian TV channels. It was both fascinating and saddening to cover this topic during the 2022 Q2 edition of *Infosecurity* Magazine.

Ukrainian cyber-defenses have proven incredibly robust to these relentless attacks, showing a resilience developed over many years of Russian-backed cyber-attacks, most notably NotPetya. The world can learn from Ukraine's experiences when looking to enhance their own cyber-defenses, Lindy Cameron, the UK National Cyber Security Centre's (NCSC) CEO, argued in a speech to the Chatham House security and defence conference held in September. This is a vital message as the conflict is likely to put organizations in the West, especially those implementing sanctions against Russia, at greater risk of sophisticated nation-state backed cyber-attacks, both now and in the future.

Such issues provide another reminder, if needed, of the critical importance of cybersecurity for our future lives and prosperity. At *Infosecurity*, we have been at the forefront of covering futuristic cyber-threats and long-term solutions over 2022. Most notable is the threat posed by advances in quantum computing, which experts believe will be capable of breaking existing encryption methods in the next five to 10 years. The race is now on the develop, and implement quantum-secure encryption technologies before 'Q Day' occurs, and there are a number of initiatives taking place in this space, including the National Institute of Standards and Technology's (NIST) project to develop a post-quantum cryptographic standard.

I have also relished the opportunity to analyze the UK government-backed Digital Security by Design (DSbD) initiative, an ambitious program designed to secure underlying computer hardware. Enabling the development of innovative technologies to secure computer hardware, would, in theory, prevent the majority of vulnerabilities from ever occurring, thereby removing a major headache for security teams. It is a huge challenge to a) create new hardware systems that are secure by design and b) replacing existing systems with such technologies. A core component of DSbD is ensuring substantial awareness and collaboration across all relevant stakeholders – government, industry and academia – to make this vision a reality. This is an approach I am seeing discussed more and more generally within the industry. There is a growing appreciation that cybersecurity is too difficult, and important, to be left to a few IT experts. Instead, it requires understanding and input from all, including individual users being aware of how insecure behaviors create risks for them and their employers. This reality has been acknowledged in the UK's current national cyber strategy, which promotes a 'whole-of-society' approach to cybersecurity.

As we approach the end of 2022, the cybersecurity industry continues to face a major cyber skills shortage. This is an issue that will not be solved overnight and requires a multi-faceted approach. Anecdotally, I have been thrilled to hear increasing acknowledgment of the need to create new pathways and hiring practices, thereby encouraging a far wider pool of talent to enter the sector. For example, global certifications organization (ISC)² introduced an entry-level cybersecurity certification earlier this year, providing a new option for those seeking their first role in the industry, which often proves so difficult to get due to unrealistic demands on applicants.

Therefore, I believe cybersecurity is in a bitter-sweet moment. The scale and sophistication of cyber-threats, exacerbated by growing nation-state attacks, is like nothing we have seen before. Yet, as the saying goes, necessity is the mother of innovation, and the industry is increasingly coming up with new ideas and ways of doing things in response to the immense challenges, which is fantastic to see.

Along with my colleagues in the *Infosecurity* Magazine team, I look forward to covering and supporting innovative ideas and technologies to help secure cyberspace, next year and beyond.

Thanks for reading this issue,

James Coker

DATASHUR® BT

Smartphone authenticated, hardware encrypted USB flash drive.

MANAGE YOUR DATA, **ANYTIME, ANYWHERE.**

Complimentary 3-month datAshur BT Remote Management license with every datAshur BT purchase.

Terms and Conditions: Receive a 3-month subscription to the datAshur BT Remote Management Console for Free with every datAshur BT purchase. Promotion valid from 31/10/2022 to 31/01/2023.

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

iStorage®
Innovation made **simple.**