Infosecurity® Magazine

Q2, 2023 / Volume 20 / Issue 2

Untangling IoT Regulation and Security

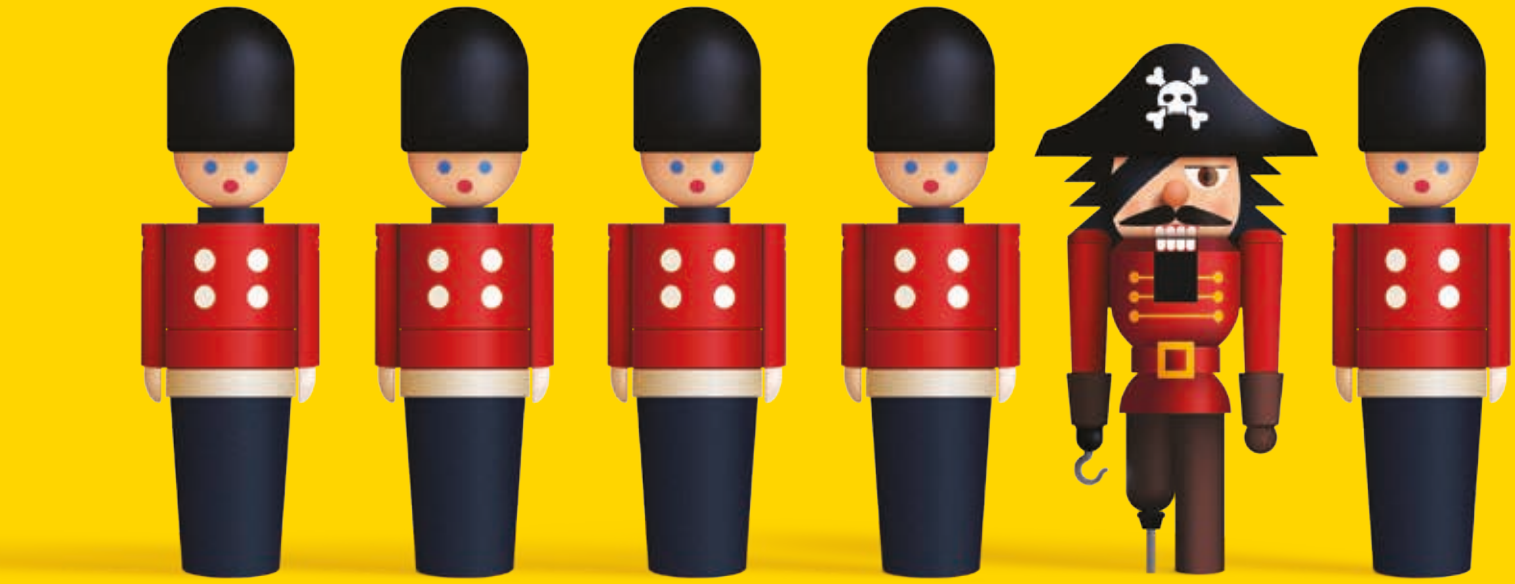
INFOSECURITY EUROPE SHOW PREVIEW

SECURING THE SUPPLY CHAIN

DIGITAL TRANSFORMATION DRIVING RISK

An oversight?

That's all it takes to cost you your organization.



Safeguard your business with ManageEngine's cybersecurity solutions.

ManageEngine 20 YEARS

Our solutions

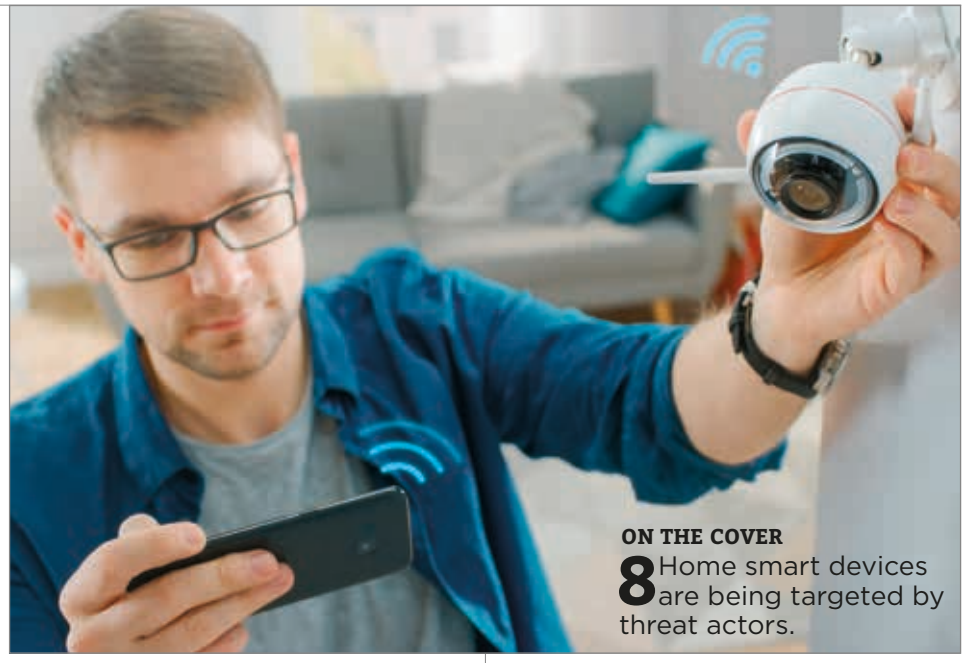
Cloud security | Identity and access management

Security information and event management | Endpoint security

Network security | Data security

www.manageengine.com/cybersecurity

CONTENTS



ON THE COVER

8 Home smart devices are being targeted by threat actors.

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 Magazine

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

INFOSECURITY GROUP

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

Group marketing manager **Julia Clarke**
julia.clarke@rxglobal.com

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


Infosecurity® Europe
20 - 22 June 2023, ExCeL London
One month to go
Keep up to date on the latest innovations
Connect with the brightest minds
Get hands-on with the technology
Benchmark your solutions and strategies
Register at www.infosecurityeurope.com

From the Editor...

Welcome to the second edition of *Infosecurity* Magazine for 2023. This special edition includes the Infosecurity Europe Show Preview that has been carefully curated by me and the editorial team. This gives you top tips on how to navigate this year's event and what are the must-sees at the conference sessions and expo.

I am truly excited to be heading up the editorial team at this year's Infosecurity Europe and am looking forward to meeting many members of the cybersecurity community there. Infosecurity Magazine will have our own stand (#L90) that you can visit and speak to the team about our digital offerings, our news output and what we're planning for the rest of 2023.

Infosecurity Europe is the largest gathering of information and cybersecurity experts in Europe and I'm truly excited to be a part of this year's event.

Head over to page 18 to find out more from the show preview.

Now, on to what is included in this second edition of the magazine for 2023. First, *Infosecurity* Magazine's Kevin Poireault reports from the UK House of Commons where (ISC)² and the Royal United Services Institute (RUSI) launched a new report exploring cyber policy and regulation.

It comes as no surprise that greater collaboration was one of the main calls to action for governments that are currently pursuing new cybersecurity legislation.

In the report, titled *Global Approaches to Cyber Policy, Legislation and Regulation*, researchers identified various challenges with shaping cyber policy across six jurisdictions, including the need to tackle the shortage of skilled cybersecurity professionals and the growing importance of protecting critical national infrastructure (CNI). Read more on page 8.

Kevin also investigates IoT regulation in this edition and examines who is leading in this field as smart devices start to dominate both our homelives and businesses. Shockingly, 54% of organizations suffer from attempted cyber-attacks targeting IoT devices, according to CheckPoint.

Back to Basics

We still celebrate World Password Day on the first Thursday of May, and James Coker has taken time to speak to cybersecurity experts about the state of password advice today. The main takeaway being that there is significant confusion over password advice, which is ultimately adding to poor password practices being a top security concern for organizations.

In his piece, James examines the advice on passwords dished out by the likes of the Information Commissioners Office (ICO), National Cyber Security Centre (NCSC) and US National Institute of Standards and Technology (NIST). One thing they have in common is that they all presume to take different approaches. How to achieve consistent authentication guidance is also discussed in the article.

James also undertook our profile interview for this edition – with the renowned Sian John MBE, Director of Security Business Development and Strategic Growth for Microsoft. Here, we find out more about Sian's fascinating journey in the industry and her prominent roles at government and non-profit organizations in cyber.

Next, SolarWinds, yes people are still talking about it – including Kate O'Flaherty who investigates what organizations have learned three years on from the incident. This cyber-attack put the supply chain issue in full focus, but companies are still grappling with how to ensure their third-parties are secure.

Speaking to cybersecurity professionals, Kate reports that a change is starting to happen but there is still much to be done to ensure supply chains are secure.

The exploitation of weaknesses and vulnerabilities within third-party suppliers is still on the agenda for many threat actors wishing to deploy the latest malware and ransomware to larger organizations. IoT rears its head again as something that is likely to see unforeseen supply chain risks.

The discussion then moves onto the software bill of materials (SBOM), something that has garnered much debate since being laid out in President Biden's National Cybersecurity Strategy, published in March 2023.

Finally, Phil Muncaster investigates why digital transformation is driving a wave of new risks in the application programming interface (API) world. With more organizations now using APIs, a lot of traditional web application security tools are falling short and leaving holes in protection. In his feature article, Phil explores how firms can take action and carry our good API governance.

With this, we hope we have just a slice of the cybersecurity landscape covered for you. If you'd like to learn more about other topics like threat intelligence, cloud security, the dark web, the latest vulnerabilities and enterprise-level security make sure you head over to the website infosecurity-magazine.com where you'll find news, features, whitepapers, webinars and our online summits.

Happy reading and we look forward to seeing you at Infosecurity Europe 2023.

Beth Maundrill
Editor

END

CYBERSECURITY REGULATION REQUIR STRONGER COLLABO

A new report by (ISC)² and British think tank RUSI examines global approaches to cyber legislation across six jurisdictions. *Kevin Poireault* was at the launch event in Westminster on April 26, 2023

As cybersecurity policies and regulations evolve rapidly around the world, greater collaboration is necessary to ensure more robust and resilient frameworks to support shared learning and best practices, according to (ISC)².

The international cybersecurity non-profit has led new research in collaboration with the Royal United Services Institute (RUSI), a British think tank, examining cybersecurity legislation and regulation within the UK, the US, Canada, the EU, Japan and Singapore.

The report, titled *Global Approaches to Cyber Policy, Legislation and Regulation*, was published on April 27, 2023.

It is the result of "a first-of-its-kind comparative work, pushed by the proliferation of new cyber regulation – and the fact that more is on the way," Clar Rosso, CEO of (ISC)², said during a launching event that took place at the House of Commons, on April 26, 2023.

"We picked countries where (ISC)² had the densest concentration of members, but also which we thought have the most robust cybersecurity policies," Rosso told *Infosecurity*.

Tackling the Cyber Skills Shortage at Scale

RUSI and (ISC)² researchers identified various challenges shaping cyber policy across all six jurisdictions, including the need to tackle the shortage of skilled cybersecurity professionals and the growing importance of protecting critical national infrastructure (CNI).

While these two priorities are shared by all six jurisdictions analyzed, the report provides valuable insights on the different approaches these countries take to solve them, Rosso said.

The cyber skills gap is a prime example of a challenge that all countries face, she said. "There are 14,000 open cybersecurity positions in the UK and (ISC)² even estimates a gap of 58,000 cyber roles in the country, while the US is probably in need of hundreds of thousands of cyber roles – and the same goes in other regions."

Initiatives like the Cyber Skills Academy, an EU scheme launched on April 18, 2023, to "boost the EU cyber workforce," is something that could inspire the UK and other ally countries, she added.

"We need to know what other countries are doing – and not only those analyzed in the report. During GISEC Global [an event that took place in Dubai on March 14-16, 2023], I learned that, in the UAE, over 70% of students in STEM are women, and many are moving into cybersecurity jobs. We need to find what attracted them to those programs and we need to model and replicate that around the globe," she insisted.

"With a global 3.4m people cyber skills gap and 95% of small businesses with no cybersecurity professionals at all, you can't be moving people one by one into cyber jobs, you need to do that at scale. As of now, no government has answered that challenge at scale yet," she told *Infosecurity*.

Collective Defense

To do so, governments will also need to work together rather than just compete for hiring cyber workers. "I don't think we're competing. I think that, if our cybersecurity agencies embrace the concept of 'collective defense', which encompasses information, best practice and experience sharing, all our national cybersecurity industries can actually benefit," Rosso said.

ES RATION

Pia Hüsch, a research analyst at RUSI and the report's principal author, said that by bringing together insights from different jurisdictions and stakeholders, the report also shows the importance of cooperation between private and public stakeholders and that policymakers increasingly seek harmonization of cyber policy.

"The report therefore draws crucial attention to the need to better understand which policies are effective in increasing cyber resilience and how they impact businesses and the cyber workforce implementing them," Hüsch added.

The research led by RUSI comes at a critical time, Rosso noted. "As cyber-attacks made more and more headlines, we have also seen increasing cyber policy, legislation, regulation all around the globe. We knew that, if we don't start on a path of standardization, harmonization, we're going to end up with an ineffective, complicated patchwork of regulation around the globe. We need cybersecurity professionals focused on defending our information systems, not navigating regulations."

"It's important, as we see a proliferation of cybersecurity regulations across the world, to find out what some of the leading jurisdictions are doing," Clar Rosso, CEO of (ISC)², said at the House of Commons, in London, on April 26, 2023.

More than just a comparative work, (ISC)² hopes this report can be the basis for ally countries to adopt "a proactive, rather than reactive, approach toward cybersecurity policy and collaborate across borders, industries and sectors to establish common standards, protocols and best practices. For instance, nations are beginning to realize that they need to share intelligence with each other – and Russia's invasion of Ukraine has to some degree accelerated this process," Rosso told *Infosecurity*.

(ISC)² is ready to be an enabler to facilitate cooperation between policymakers she added. "Because we are in so many countries, we have a line of sight that you don't have if you're on the ground. We can start helping connect dots and encourage the conversations that could take a little longer organically. We'll continue to do it; we're committed to this for the long term."

The research was conducted from December 2022 to March 2023 and was primarily based on a review of existing literature about policies enacted or proposed within the six jurisdictions between 2019 and 2023.

The report's launch came a week after the CYBERUK 2023 conference, where (ISC)² called for cross-industry support to launch 100,000 new cybersecurity careers in the UK END

IOT DEVICES AWASH WITH NEW REGULATION

After a long time spent in a cybersecurity legal vacuum, providers of internet-of-things devices will soon be required to implement some security measures. *Kevin Poireault* investigates how this will impact the market

"There's always an option to let us leak your data." This was the message shared by ransomware group ALPHV, also known as BlackCat, which claimed to have breached the popular security camera company Ring, owned by Amazon, in March 2023. While Ring has denied the breach, some security experts, including those behind the malware repository VX-underground, confirmed it.

This is not the first time Ring has been the victim of a cyber-attack. A 2019 hack led customers to file a class action lawsuit against the company the following year.

With other camera-makers, such as surveillance firm Verkada, having also fallen victim to cyber-criminal activity, the live-viewing device has become the unintentional standard bearer of an easy-to-hack IoT market.

In an April 2023 survey, cybersecurity firm CheckPoint found a 41% surge in the average number of weekly attacks targeting IoT devices per organization in the first two months of 2023 compared to 2022.

"On average, every week 54% of organizations suffer from attempted cyber-attacks targeting IoT devices," the report adds.

This emerging threat not only affects organizations using the devices but is also detrimental to IoT manufacturers. In an article published in April 2023, McKinsey & Company claims: "By 2030, the IoT suppliers' market is expected to reach approximately $500bn in a baseline scenario. However, in a scenario in which cybersecurity concern is completely managed, executives would increase spending on the IoT by an average of 20-40%, [which] implies that the combined total addressable market value across industries for IoT suppliers could reach the range of $625bn to $750bn."

Cybersecurity vendors, like CrowdStrike, Claroty and Palo Alto Networks, among others, are launching new offerings dedicated to securing IoT devices and new IoT security-specific startups have emerged, such as NetRise, which raised $8m in April 2023 to grow its extended IoT (XIoT) security platform.

However, these products won't solve all security issues IoT devices have, and a deeper problem lies with IoT manufacturers, Erik Brenneis, CEO of Vodafone IoT, claims. "Many of them don't worry too much about security," he tells *Infosecurity*.

Florian Mendel, one of the developers of ASCON, the encryption and authentication algorithm for lightweight IoT devices that was recently selected to be standardized by the US National Institute of Standards and Technology (NIST), concurs: "Today, no one really wants to pay for security until it's too late."

> ***"Today, no one really wants to pay for security until it's too late"***

Joel Demarty, CTO of IoT and automotive at Thales, urges countries to adopt stronger regulations to change the narrative. "Most IoT suppliers don't spend what's needed to build secure-by-design devices. Regulating this space is today the only way that they gear up for the challenges ahead."

Leading the Way in the USA

As Demarty implies, IoT is still a largely unregulated market, especially regarding security measures, except, perhaps, in the defense, automotive and healthcare industries. In 2020, the UN Economic Commission for Europe's (UNECE) World Forum for Harmonization of Vehicle Regulations (WP.29) introduced regulatory measures to require incident response plans or regular software updates, for instance.

In the US, the 405(d) project, a collaborative effort between industry leaders and the US federal government to align healthcare industry security practices, has also developed guidelines, practices and methodologies to strengthen the healthcare and public health sector's cybersecurity posture.

Nevertheless, most of them are 'mere' regulatory frameworks, thus not enforceable, Stephan Goldberg, VP of Technology Alliances at industrial cybersecurity vendor Claroty, says. "In the healthcare sector, most cybersecurity regulations are advisories – almost nothing is formally required," he recalls from his time at Medigate, acquired by Claroty in January 2022.

Some general cybersecurity regulations, such as the EU's 2018 Network & Information Systems (NIS) directive and 2019 Cybersecurity Act, have "laid the foundations of a desired state of security embedded in all devices, IoT ones included," according to Tom Klein, senior director of IoT business development at identity certificate provider DigiCert. But again, they do not include any strict requirements regarding IoT devices.

+41%

The average number of weekly attacks targeting IoT devices per organization in the first two months of 2023 compared to 2022.*

Now, some governments decided it was time for a change. In the US, the IoT Cybersecurity Improvement Act, signed by then President Donald Trump in December 2020, was the first significant IoT-specific law in the world.

It called for the definition of standards, guidelines and minimum-security requirements that IoT devices will need if connected to federal government information systems and outlined a requirement for a vulnerability disclosure process, which will clear the way for ethical hackers to test IoT devices used in federal government systems for vulnerabilities and report them responsibly.

54%

The average weekly share of organizations which suffer from attempted cyber-attacks targeting IoT devices.*

Those measures, along with others defined by the bill, are to be controlled by NIST and deployed by the Office of Management and Budget (OMB).

However, this first IoT Act had a limited reach since it only affected IoT devices used by US federal agencies and exempted those used in national security systems.

That same year, the US states of California and Oregon preceded the federal government with their own legislation. These two laws, respectively, California's SB-327 and Oregon's HB 2395, mandated a few basic measures, such as "all IoT devices need unique passwords" or "reasonable security is required." They also are very clear that, in case of a security breach, the manufacturer, not the retailer, is responsible – unless the device has been modified by the user, in which case responsibility lies with the latter.

More importantly, they highlighted some of the existing bottlenecks in drafting IoT security legislation: "The requirement for 'reasonable security' is not clear because it is not defined," IoT security firm BG Networks argued in a blog post published in 2021.

First Sanctions in the UK and EU

In 2021, the UK introduced the Product Security and Telecommunications Infrastructure (PSTI) Bill, one of the first national laws regulating almost all consumer IoT devices – connected vehicle devices, smart meters and medical devices are not concerned – based on a 2018 Code of Practice. Amongst a series of measures, the PSTI Bill, passed in 2022, introduced three critical changes for IoT security:

- The prohibition of marketing devices with default passwords that are easy to guess
- The introduction of a vulnerability disclosure policy for IoT products so that security researchers and other members of the public can notify manufacturers of any issues they discover
- More transparency and communication between manufacturers and consumers about whether security updates are provided, and the amount of time they are provided for

It was also the first legislation to introduce non-compliance fines, of up to £10m ($12.5m) or 4% of global annual revenue, as well as up to £20,000 ($25,000) a day in the case of an ongoing contravention.

While UK officials called the text "world-leading legislation" when it was adopted in 2022, the bill was criticized

*Source: CheckPoint

for failing to require patch management, among other shortfalls.

The EU's new Cybersecurity Resilience Act (CRA), while very similar to the UK's PSTI Bill, includes the requirement for IoT manufacturers to have mechanisms to fix any flaws discovered in their devices for up to five years after they have been sold to consumers.

The proposed draft of the CRA presented in September 2022 stated that each connected device and the software it embeds must be certified. For 90% of the products, manufacturers will be able to assess them themselves. The intervention of a third party will be mandatory for devices considered critical, such as routers or operating systems.

Failure to comply with safety standards may result in a fine of up to €15m ($16.5m) or 2.5% of annual worldwide turnover. In addition, national authorities will also be able to ban the marketing of a device on European soil.

$500bn

The expected value of the IoT market by 2030 in a baseline scenario.**

In its first draft, the CRA foresees that open-source software developed or provided "in the context of a non-commercial activity" will not be concerned by these new obligations. In other words, their editors will not be worried if a security flaw is detected in a connected object.

This wording has been criticized by some open-source community members, including the Linux and Eclipse foundations, for being confusing. They signed an open letter in April 2023 to ask for more clarity.

A Market Differentiator

For now, the US has chosen a different path than the UK and the EU in its plan to secure IoT devices. Following Joe Biden's 2021 executive order on Improving the Nation's Cybersecurity, the federal government mandated the NIST to work on a labeling program for consumer IoT devices.

This program, officially announced in May 2023, is inspired by the Energy Star, a US federal trust scoring scheme to promote energy efficiency.

"If you look at sections 3.2 and 4.5, particularly, the security labeling program will emphasize the need for immutable identities, that can't be spoofed, in accessing IoT devices, which is a great step forward," Klein praises.

$625bn-$750bn

The expected value of the IoT market by 2030 in a scenario with secure-by-design IoT devices.**

While the idea of a security score may sound relatively lax compared to European legislation, Lorrie Cranor, director of Carnegie Mellon University's CyLab, hopes that it can flip the script and turn security from a constraint to a market differentiator. Cranor has been working on a security labeling framework for IoT devices for several years at CyLab.

"There are a few paths for adopting a security scoring system in the US. First, Congress could pass laws that include the provision requiring manufacturers to implement it – and there have been proposals in the past to do this in the US. Second, we could be influenced by other countries' legislations, just like the EU's General Data Protection Regulation (GDPR) influenced several US states to adopt data privacy laws. But my hope is that manufacturers will see this as an opportunity and that we're going to start a race to the top rather than the bottom," she said in Claroty's April 2023 Nexus podcast.

Klein also has high hopes for the EU's CRA and the US labeling program. "There is a real momentum for IoT regulations, with other countries, like Japan, Singapore and Australia, also working on their own laws. My only fear is that these initiatives keep being scattered and that countries don't cooperate in developing more consensual standards," he tells *Infosecurity*.

Klein's fear may already have started to be realized, as a British parliamentary committee scrutinizing the impact of the CRA in the UK showed in an April 2023 report that, although similar, standards introduced by UK's PSTI Bill could not be translated into the ones pushed by the EU legislation.

"Even if the substantive cybersecurity requirements for a particular device were the same in the UK and the EU, there would still be administrative hurdles," said the committee, as there is no agreement between the two jurisdictions – and may well not be until 2025, when the EU/UK Trade and Cooperation Agreement following Brexit is planned to be reviewed.

Cyber-criminal groups may have no frontiers, but cybersecurity legislators still do. Removing them will itself be a challenge – and one that must be addressed quickly if we want to reverse the trend and stop seeing all sorts of cameras and other connected devices being hacked END

In an ideal world, all IoT suppliers would...

- Respect internationally recognized standards
- Conduct conformity assessment (self- and third-party)
- Conduct regular testing (e.g. compliance, penetration tests)
- Provide product lifecycle management and support
- Conduct software and firmware update/patch
- Conduct system monitoring and audit
- Offer traffic monitoring and/or blocking
- Maintain system or technical logs
- Maintain a software bill of materials (SBOM)
- Offer alerts (e.g. intrusion detection, abnormal access requests)
- Provide encryption
- Allow pseudonymization or anonymization
- Not use default passwords

Source: IoT Security Foundation

***Source: McKinsey & Company*

TWO EXPERTS GO HEAD TO HEAD

Point

Has the Ransomware Threat Reduced?

Yes

Jake Moore

Global Cybersecurity Advisor, ESET

Jake's current role revolves around offering unbiased cybersecurity support and advice to organizations. He previously worked for Dorset Police spanning 14 years, primarily investigating computer crime in the Digital Forensics Unit.

@Jake_MooreUK

There are several possible reasons for the decline in ransomware payments and attacks since 2021. These include greater collaboration and action by law enforcement agencies across the globe, disruptions caused by the conflict in Ukraine and increased regulations limiting the amount of ransom payments that reduce the potential financial gain for cyber-criminals.

Ransomware was once the go-to cyber-attack vector for many criminal groups and bad actors, but it was essentially a victim of its own success. The more organizations that had to pay out eye-watering amounts to cyber-criminals to try and recover their data, the more this paved the way for those companies (and watchful others) to double down on protection.

In previous years, threat actors would create a simple campaign, target a few employees and wait for the payload to erupt, encrypting all the data of a company of any size. Many organizations would have no idea what was happening and even require the helping hand of the hacker to walk them through the reality of what has hit them. All the hackers then had to do was wait for the unsuspecting and panicking victim to pay for the decryption key.

But, as more companies were used as guinea pigs and big corporations made the news after being caught up in a critical state, criminals were forced to work harder to change tact by stealing some data first for insurance.

Resilience in the Face of Attacks

Prevention measures, including better backup policies with restore functionalities don't have to break the bank, whereas ransom demands can. It might have taken years, but we are starting to see the curve level off as affected organizations slowly start to say 'no' to criminal demands. Unless cyber-criminals get their hands on personal data to use as a bargaining tool and threaten to release it, it is understandable that criminals are increasingly looking at other creative ways to succeed financially, such as cryptojacking.

Stealing personal and confidential information on employees and customers was once seen as the end of a company, but as ransomware attackers shuffled sideways to steal information as part of the default attack, more organizations could brush it off as a 'necessary evil' part of the business model. With this seen as normal as the attack itself, along with weak threats from the Information Commissioner's Office (ICO), organizations pivoted to spend their money more wisely on prevention methods, insurance and faster restoration speeds.

Since the extremes of 2021, we have seen a huge shift in how attackers are using their once loved and trusted tool. The numbers are dropping and it even feels like a slight win for the little guy who rarely enjoys a victory in the war on cyber.

Refusal to Pay

Ransomware has forced companies to add these robust measures to withstand these attacks, but cyber-criminals are very in tune with their victims and fully understand the defenses they come up against. Companies were once very much specifically targeted by criminals in their attacks and the hackers would do their homework in order to leverage the highest ransom, even making it feel personal. Now the ESET *Threat Report* telemetry indicates that scammers are acting opportunistically and often attack like a scattergun.

In this approach, however, hackers are finding themselves caught up negotiating with organizations that simply cannot afford to pay any ransom at all, such as schools or hospitals.

In large organizations, ransom negotiations are extremely difficult as both sides have good game plans and ulterior motives. Victim organizations are desperately looking to extend the time frame before payments are demanded, while criminal groups aim to find the sweet spot in which a ransom amount is viable.

However, as ransomware is now considered a relatively old form of cyber-attack, both sides often know how the other thinks, which can have both advantages and disadvantages. Without wanting to see any information spilled onto forums and other criminal trading platforms, even negotiating over time can upset attackers into releasing stolen data.

By not paying a ransom, it sends a very strong message to the criminal underworld that companies will not succumb to such demands anymore and together they are more powerful. This has had a profound effect across every industry and proverbially sticks two fingers up at threat actors who are left angry and will release what they have. The clear financial motivation is stated in the demand notes but not responding or negotiating could pave the way for less ransomware attacks to take place in the future.

It is anticipated that throughout the rest of 2023, the already saturated ransomware market will become even more intense and cut-throat. This will be partly due to ideological conflicts and disputes arising among different ransomware groups. As defenders, we need to remain optimistic that such conflicts will cause the threat actors to lose focus and commit errors that can be exploited to develop decryptors and, ideally, result in their capture and prosecution END

Counter-Point

No

Chaos, destruction and financial gain are the aims of ransomware, which is why it has increasingly made headlines in recent years.

While increased law enforcement activity and collaboration between allied governments and agencies in taking down the likes of REvil and Lapsus$ has made an impact, the data shows that ransomware is not on the decline. According to the NCSC, ransomware has been the greatest cyber threat facing the UK since 2021 and it has not decreased in the past year. The nation's cyber guardian has had to deal with record numbers of ransomware incidents, 18 of which required a national-level response.

Australia's move to chair a new International Counter Ransomware Task Force, an effort under the US-led Counter Ransomware Initiative made up of 36 nations and the EU, shows the perceived threat is not diminishing. This is a strong signal of ransomware's prominence and pervasiveness worldwide – not of a waning threat.

Kept Under Wraps

When analyzing ransomware threats, it's important to remember that attacks are often under-reported to the authorities and the public.

Fear of reputational damage has motivated some to keep quiet. Also, the imposition of fines for paying ransoms or not protecting sensitive data could lead to more organizations not reporting an incident.

The recent attack on Australia's largest health insurer, Medibank, brought increased scrutiny as the personal data of nearly 10 million people was leaked. A class-action lawsuit has since been filed claiming Medibank failed to protect its customers' privacy. This is attention that no business wants, and many companies are not in a position to take the financial hit and pay both the ransom demanded by the criminals and fines.

Sowing Chaos in the Public Sector

These attacks are not always motivated by money. Some groups revel in the chaos they create and the notoriety that follows. A growing number of threat actors are not adhering to so-called ethical practices, and we are seeing hospitals and schools targeted. Organizations of any type and size can be affected – from small businesses to the Colonial Pipeline in the US and giant multinationals like Toyota and Okta.

Data leaks stemming from these attacks can have longer-lasting effects for individuals. There is also a big cost and burden to the digital economy when operators feel the strain and people believe they can't do business online safely.

> ***"When one group goes down, it leaves a void for others to fill"***

Our public services and businesses are under increasing pressure to protect themselves against ransomware threats that evolve and change with the technology landscape. While software and hardware manufacturers are getting better at pushing patches and updates to their customers, busy teams can struggle to keep up. The burden of prevention and stress around possible attacks is a growing concern for organizations. Fallout from an attack can slow productivity and add pressure to employees. The wellbeing of their employees, and the trust of their customers, is at stake for these organizations.

Filling the Void

Great strides are being made against the ransomware threat and governments should be applauded. While agencies like the NCSC, CISA and Europol have taken down several notorious ransomware groups, it's often a short-term solution as the infrastructure and assets have re-emerged elsewhere. When one group goes down, it leaves a void for others to fill. Some groups have the funds to rebrand many times over.

What's more, you don't even have to be an expert to operate in this field anymore. Ransomware-as-a-Service (RaaS) kits are increasingly commoditized, making it easier to carry out attacks. They're easy to find on the dark web and are advertized like any consumer product on the regular web. This business model is one to watch as attacks remain persistent and damaging, with private organizations and public services constantly scrambling to protect themselves against the changing shape of the threat.

Opening Pandora's Box

Significant progress has been made by the authorities in taking down groups and driving down the revenue they make from their attacks. Some may argue this is why the ransomware threat is diminishing.

Yes, we are making great strides against this threat. Governments are trying new policies, collaborating more deeply, and the private sector is responding too. This is driving down the revenue these gangs are getting from their attacks.

But the lid is off of Pandora's box. Cyber-criminals are always seeking out vulnerabilities they can exploit to make a dollar or grab a headline and the impact on the way we work and live online is significant and enduring END

Kim Wiles

Government Cyber Services Expert and Product Manager, Nominet

Kim Wiles is a government cyber services expert at Nominet, developing solutions to protect public services at scale. ***@NominetCyber***

CONFUSION OVER PASSWORD ADVICE ADDS TO TOP SECURITY RISKS FOR ORGANIZATIONS

The plethora of recommendations around password practices is causing confusion and stress for users. *James Coker* investigates

The fact that password security remains a relevant topic is a source of frustration to many cyber professionals, particularly with so many viable alternative authentication methods, such as biometrics, readily available.

Poor password practices still present enormous security risks for organizations, with Verizon's *2022 Data Breach Investigations Report* finding that stolen credentials led to nearly 50% of attacks in 2021.

Confusion For Users

Given the level of risk around password compromise, relevant organizations – including government agencies, independent organizations and large tech providers – have issued various guidance and mandates around password practices.

However, this has led to a wide variety of advice being issued. For example, in the UK, the Information Commissioners Office (ICO) advises a minimum of 10 characters in passwords, whereas the National Cyber Security Centre (NCSC) recommends a minimum of eight.

In addition, some authorities, like the ICO and the US National Institute of Standards and Technology (NIST), say special characters should not be mandated, but bodies like HITRUST do have this requirement.

Sarb Sembhi, CTO at Virtually Informed, tells *Infosecurity*, "The advice we're given has never been consistent and is changed a lot."

This has ultimately resulted in confusion for the end user.

Outdated Practices

Research over the past few years has also suggested that a simpler approach to password policy is more effective as it makes users less likely to bypass controls.

Jessica Barker, CEO and co-founder of Cygenta, says: "The UK NCSC and NIST changed their guidance to acknowledge that asking people to repeatedly change their passwords actually leads to people using weaker passwords."

Another approach used by the NCSC to simplify password practices is the three random words recommendation, which it views as more effective than using complex combinations for passwords.

Taking the Pressure Off Users

While bodies like the NCSC and NIST are renewing their approaches to password policies, many organizations are still placing outdated requirements on users, such as using a mixture of letters, numbers, and special characters to compose passwords.

"One issue that many of our clients face is in terms of compliance with regulations, with different rules and expectations, some of which go against the good practice recommended by the UK NCSC and NIST," says Barker.

Although well-meaning, Brian Honan, CEO of BH Consulting, notes that orthodox advice often has the opposite effect on security: "When you take a logical look at that advice you realize how bad it is and how difficult it actually is to follow. This in turn leads to people to reuse passwords or use variants of a password that they believe to be secure."

Sembhi also believes the obligations such policies place on users is an additional cause of stress, potentially contributing to mental health problems in workers.

"It's the vendors that need to get it sorted, not the government telling users to get it sorted," he states. "That is fundamentally wrong and there needs to be some sort of standard approach that vendors should be asked to follow."

Authentication as a Whole

Both Honan and Sembhi believe there must be a more unified approach to guidance encompass authentication as a whole, primarily aimed at vendors and organizations.

"The concern I have is the focus is still on people creating secure passwords with little or no messaging being given on the use of additional resources such as MFA and the use of password managers," says Honan.

Guidance needs to recognize that different forms of authentication are better suited to different types of devices and systems, says Sembhi. For example, biometric authentication works much better on mobile phones than desktop computers, while PINs work well on Microsoft Windows.

He believes the use of flow charts and maps will help provide these insights. "It should be simple because they're rules we've talked about for years, we've just never put them down on a piece of paper," comments Sembhi.

Achieving Unification

The path to unified standards around authentication must be industry-led, according to Sembhi. However, he does not believe an ISO standard will be appropriate in this instance "because small organizations won't be able to comply with it."

Instead, "it needs to be an open standard that everyone can use and view," he commented.

What's key, adds Sembhi, is that developers have uniform guidelines to follow to build in authentication approaches into platforms.

The first stage is to set out a proposal, and then invite discussions among the industry to adapt and refine via conferences and other mediums.

"Until something is on the table, no-one's going to initiate," notes Sembhi.

Having multiple recommendations from different organizations on password practices, much of which is outdated, is creating confusion and difficulties for users. A unified approach to authentication more generally, aimed at building best practices into systems by design, will be crucial to stemming rising breaches going forward

END

Infosecurity® Europe

20 - 22 June 2023, ExCeL London

Show Preview

Register at www.infosecurityeurope.com

RX In the business of building businesses

SolarNet | Stand F84

Come and see us for a demo in the discovery Zone

Our Mission

SolarNet offer a comprehensive consultancy service within the IT and Cyber Security industries. We have a long and varied experience within the software development, testing, telecoms, IT and cyber security industries. The services offered are tailored to each customer's individual needs to help them to meet their goals.

SolarNet has established partnerships with key technology providers. These broaden our service offerings with technology that complements our own capabilities, whether that be in IT consultancy, cybersecurity, or orchestration and automation.

By working closely with our partners, we can deliver the very best service, to the highest possible standards, which our customers have come to expect from us.

Our Services

Cyber Security

Protecting your assets against cyber threats is something we can help you with minus the jargon!

IT Consultancy

Our consultancy service will help your business gain clarity on all things IT, don't get bored down with acronyms!

SOAR Consultancy

Security Orchestration Automation and Response are not just buzz words, see how we can help you!

Testing & Automation

With over 25 years experience in everything testing we're positive there's something we can help you with!

Our Founder

Mike Smith, Executive Director

"We continually provide Innovative thinking, combined with integration of the latest technologies through our partner network, to give the best experience to our customers."

www.solarnet-comms-ltd.co.uk | info@solarnet-comms-ltd.co.uk

WELCOME

Welcome to the Infosecurity Europe 2023 event preview. The editorial team and I have curated this content to help you, the attendees at this year's event, make the most out of your three-day visit.

For the past 12 months the cybersecurity world has been tackling new and evolving threats, from nation-state backed campaigns to the security impact of new AI tools like ChatGPT.

With a keynote programme featuring some of the foremost experts in cybersecurity, Infosecurity Europe will deliver key insight and the latest industry information, designed for C-level information security professionals.

Whether you want to stay on top of the latest trends, are facing data regulation challenges or are looking to implement new policies across your organization, there is much to be learned from this year's event.

One thing myself and the team are extremely excited about is this year's gold-standard opening keynote. A session set to inspire and motivate, four-time Olympic gold medallist Michael Johnson will offer unparalleled insights on how to perform against competitors, stay agile under adversity and consistently pursue and achieve excellence against the odds.

Michael's keynote is a must-see to inspire your team and solidify their purpose, regardless of their specific expertise or specialism.

Michael Johnson said: "In cybersecurity, the journey to success should follow this same mentality. Having the ability to remain agile, lead and be lead, and accepting that there will always be challenges to overcome, will enable you to get over the finish line."

Considering the cybersecurity environment most organisations now exist in, I'm sure Michael's words resonate with many reading this now.

Speaking to me ahead of the event, Nicole Mills, Event Director at Infosecurity Europe said: "We are delighted to be hosting the 27th Infosecurity Europe at Excel, London, the biggest gathering of the information security industry in Europe. Cybersecurity is top of the agenda for all businesses and bringing the community together is vital to tackle today's challenges."

We always speak about collaboration as a community, and once again Infosecurity Europe will bring the community together to share innovation, learn from each other, test and benchmark solutions, build relationships, drive new business and connect with colleagues.

For the second year, the event will be heading to the ExCel London and with the city's new Elizabeth Line now in service, it is easier than ever to travel to the historic docklands area.

There is so much to do, see and explore at this year's event, including the amazing keynote line-up, new solutions from exhibitors, three-days of networking opportunities plus workshops to keep you up to date with your certifications by earning CPE and CPD credits at the event. We all know how important these certifications are to your careers.

On a personal note, it is a pleasure this year to be leading the *Infosecurity* Magazine editorial team during this year's event. We'll be bringing you daily content, including breaking news during the show and expert interviews on site, so you won't miss out on anything from Infosecurity Europe 2023.

Join us as we rethink the power of infosecurity.

Beth Maundrill,
Editor, Infosecurity Magazine

INFOSECURITY MAGAZINE EDITOR'S **TOP THINGS TO CHECK OUT** AT THE EVENT

Michael Johnson
Go for Gold! The record breaking sprinter turned pundit and motivational speaker is to share insights into how to perform against competitors and stay agile under adversity. Michael is speaking at 10:00am on June 20 at the Keynote Stage.

Keynote Stage
Featuring speakers from the sharp end of information security who are tackling information security challenges every day, the keynote programme will share best practice, case studies and real-life insight.

Women in Cyber
Hear an inspiring keynote from Danni Brooke, former undercover police officer and now Hunter on Channel 4's hit show, Hunted. It continues to be important to champion the achievements of women in cybersecurity, build bridges with allies and empower women both at the start of their careers and progressing up the ladder. As the Editor, I'm excited and privileged to be hosting this session.

Geek Street
Put your security skills to the test and participate in an exclusive 3-days Live Hacking Competition and Workshop at Infosecurity Europe 2023, courtesy of Hack The Box. Various hacking challenges await you, carefully designed to demonstrate the latest attack techniques and vectors in web, cloud, forensics, and more. It's your need-to-know showcase of the techniques you'll meet in your future security engagements. See you on Geek Street!

Innovation Showcase
This is the place to be to discover, scope out and evaluate the newest cybersecurity technologies and solutions, and get to grips with how they can be deployed. Businesses will showcase and demonstrate the exciting new products and services they have to offer.

Start-up Zone
Cybersecurity is flooded with start-ups offering the latest and greatest innovations. The start-up showcase allows you to hear from the latest information security companies at the cutting edge of technology development. Featuring bite-size presentations, discover the newest tools being developed to protect against the latest threats. A must-attend stage for infosecurity professionals that want to stay ahead of the curve.

All information in this show preview is correct at the time of going to press.

INSPIRATIONAL KEYNOTE SPEAKERS @ INFOSECURITY EUROPE

Gain insights from three leading experts in their fields from the world of sport, business, and hacking who will motivate, educate and inspire you to think about cybersecurity in a different light.

Michael Johnson

Speaking at 10am, Tuesday, 20 June on the Keynote Stage

Michael Johnson is one of the most celebrated sprinters in track and field history, holding four Olympic gold medals, eight World Championship gold medals and numerous other accolades. He's widely regarded as one of the greatest athletes of all time, but his impact goes far beyond athletic achievements.

Following his retirement from the sport, Michael has founded both Michael Johnson Performance, and, more recently, Michael Johnson Young Leaders. The latter educates and provides young people who have faced and overcome adversity with the tools to achieve a better future for themselves and their communities.

Michael Johnson has also gone on to establish himself as a leading corporate motivational speaker, and has achieved success as a television commentator and personality, working for BBC Sport since 2001.

Michael's keynote is the fast-track step to inspiring your team and solidifying their purpose, regardless of their specific expertise or specialism.

Johnson will touch on how athletes often focus on achieving short-term goals such as winning a race or tournament, but why they also need to plan for long-term success and how this applies to business through long-term strategic plans.

Matthew Syed

Speaking at 10am, Wednesday, 21 June on the Keynote Stage

Matthew Syed is an author and highly acclaimed speaker in the field of high performance. His work has influenced sport, business, education and public institutions, with explorations into everything from creativity to marginal gains and learning from mistakes.

For 10 years Matthew was England's number one table tennis player, a competitor at two Olympic Games, and a three-time Commonwealth Champion. He argues that by understanding the intimate connection between mindset and high performance, organisations can unlock untapped potential in individuals and teams, driving innovation and agility to secure a future-proofed environment.

Matthew has written six best-selling books about mindset and high performance. Matthew is also co-founder of Matthew Syed Consulting (MSC). The company has worked with an impressive portfolio of clients to build growth mindset cultures and drive higher performance in individuals, teams and organisations. Matthew Syed Consulting's cutting-edge thought leadership programme and digital learning tools are a catalyst for real and lasting change within business and the public sector.

Keren Elazari

Speaking at 10am, Thursday, 22 June on the Keynote Stage

Keren Elazari is an acclaimed security analyst, author and TED speaker. Keren will use her talk to explore the intersection of cyber conflict and politics. She will delve into the use of information as the new currency of our digital society and how those who can control it have become powerful actors, whether they choose to be heroes or villains.

Former hacker turned cybersecurity expert, Keren is an internationally celebrated speaker and analyst. Her 2014 TED talk, the first by an Israeli woman at the official TED Conference and now viewed by millions, reimagined the perception of hackers and the role they play in the evolution of cybersecurity on a global scale.

Keren has worked alongside leading IT vendors, government organisations, Big Four firms and fortune 500 companies. She will bring her experience and knowledge to Infosecurity Europe to share insights into national security and geopolitics and how they are being radically changed by digital society.

CONFERENCE STAGES

With a whopping 192 talks across three days, Infosecurity Europe has your educational needs covered. Here's what you can expect to find outside of the keynote stage at Infosecurity Europe 2023.

Insight Stage

Gain fresh perspectives on how to tackle strategic and technical cybersecurity challenges.

Join these sessions to:

- Discover and evaluate the latest developments and innovations in cyber and information security that could benefit your organisation
- Equip yourself with new strategic approaches and techniques to tackle evolving cybersecurity challenges

Who should attend?
Professionals at any level from all security areas.

Strategy Talks

Sponsor: CROWDSTRIKE

A series of inspiring presentations showcasing the latest information and cybersecurity insight, knowledge and expertise.

Join these sessions to:

- Address the strategic business challenges impacting information security
- Learn how to optimise your organisation's security posture and enhance security maturity
- Hear important thought leadership presentations on the key themes and technologies facing the industry

Who should attend?
Professionals at any level from all security areas. As these workshops cover a broad range of topic areas, each session will appeal to those with different interests, concerns and skills.

SCAN ME TO DISCOVER THE FULL PROGRAMME

Innovation Showcase

Discover, scope and evaluate new cybersecurity innovations and how they can be deployed.

Join these sessions to:

- Find out about the latest cybersecurity innovations so you can advise your company on investments
- Ask the experts technical questions so you can evaluate what technologies you need to improve your organisation's security posture
- Hear real-world applications and examples of how new technologies and solutions have been implemented

Who should attend?
Anyone with an interest in new products and innovative information security solutions.

Talking Tactics

Get practical lessons from real-life case studies to strengthen your information security.

Join these sessions to:

- Discover how to keep up with the increasing sophistication of security threats
- Get the practical and actionable knowledge to resolve specific cybersecurity challenges
- Learn how to elevate your cyber resilience through pertinent real-world case studies

Who should attend?
Professionals at any level from all security areas.

Start-up Showcase

The start-up showcase is reserved for recent companies with start-up status.

Join these sessions to:

- Hear from the latest information security companies at the cutting edge of technology development
- Discover the newest tools being developed to protect against the latest threats
- Stay ahead of the curve and hear about what's beyond the horizon

Who should attend?
Professionals at any level from all security areas.

KEYNOTESTAGE

Keynote Stage sponsor:

CROWDSTRIKE

The Keynote Stage is a peer-to-peer, thought-leadership programme, featuring speakers from the sharp-end of information security who are tackling information security challenges every day. The programme will share best-practice, case studies and real-life insight.

Infosecurity Europe's Keynote Stage deals in bleeding-edge strategic thinking for senior network defenders and information security trailblazers.

Designed to engage and inspire, our keynote conference will offer cutting-edge strategic insights and engaging cyber-power debates that will provide cybersecurity executives with groundbreaking learnings, tactical information and mission-critical content.

The vision for Infosecurity Europe 2023 is to offer cybersecurity executives the knowledge needed to navigate the rapidly transforming cybersecurity landscape.

We have selected our highlights from the programme below. Please visit https://www.infosecurityeurope.com/en-gb/conference-programme.html#/sessions for the full schedule.

TUESDAY 20 JUNE 2023 DAY ONE

STRATEGY, BUSINESS & MANAGEMENT

11:05 - 11:45

Throwdown: Have Billions of Pounds Actually Bought Us Any Cybersecurity?
Are we one press of a button away from digital Armageddon, or are we resilient enough to handle the worst of cybercrime and nation-state attacks? This give you the answer to which it is.

A Catastrophic Cyber Storm is Brewing: Catalysing Global Action to Brace for Cyberwarfare
Make sure you join this session to keep up with current affairs in the cyber world.

12:00 - 12:40

Throwdown: Security and the Business, It's Good to Talk
Listen to this lightning talk to hear about the shifting role of the security leader presented by Paul Watts of the Information Security Forum.

Panel Discussion: Emerging Threats and Trends as Cybercriminals Become More Inventive — Improving Communication Between Cyber and Business Leaders
If you are facing challenges relating to communicating security to the wider business this session will provide you with actionable advice.

12:55 - 13:30

Exercise: Tabletop Exercise: Navigating Cyber Crisis
Two PwC specialists will take you through a simulated scenario which will guide attendees through the cyber-breach response process. This tabletop exercise is a must-see for anyone looking for practical advice on how to respond to an incident.

13:45 - 14:10

"If Not Us, Then Who? If Not Now, Then When?" — Presenting Your Start-up Cybersecurity TARDIS
SMEs and start-ups are particularly vulnerable to cyber threats and in this session Plexal's director of innovation, Saj Huq will share some of the unique challenges faced by the sector that is key to innovation and economic growth. A must-see for start-ups and those working with them.

POLICY, REGULATION & STANDARDS

14:15 - 14:40

Case Study: Building an Operational Resilience
The Bank of England's Duncan Mackinnon will talk about recent work undertaken through the Cross-Market Operational Resilience Group to build the UK finance sector's operational resilience. This session promises to deliver real-world guidance from one of the UK's leading authorities.

14:55 - 15:25

The Great Disconnect: Dire Straits of Cyber Security Standards Feeding to the Hand of Cyber Criminals
Standards are not standardised in cybersecurity, but new emerging approaches are looking to tackle the disconnect. Learn more about best practices and how to fill in the gaps in standards during this session.

15:40 - 16:20

Cyber Crime Woes: Modernising our Legal Framework for the Information Age
Complying with regulation is no walk in the park for businesses and if you're facing challenges this session is for you. Hear how you can use data privacy laws and regulations to your advantage in cybersecurity.

16:35 - 17:05

Cybersecurity as an Economic Enabler and a Source for Innovation: Calling Out an Intergovernmental Regulatory Consensus
Ever noticed government regulation struggles to keep up with the pace of change? Hear about how nations are trying to deal with this challenge with new approaches that are flexible and reduce unnecessary obstacles, and where these efforts are falling short.

SCAN ME TO DISCOVER OUR SPEAKERS

WEDNESDAY 21 JUNE 2023 DAY TWO

RISK, GOVERNANCE & COMPLIANCE

11:05 - 11:30

Throwdown: Adopting 'Compliance' As a Specific Strategy to Future Proof Business Operations
Join this session to learn how to ensure your organisation is taking an approach of good security informing compliance, rather than the compliance informing security.

"The readiness is all" — Cyber Security Risks and Companies' Readiness
Many companies have accepted that they will be significantly impacted by a cyber attack within the next two years. This means readiness is key. Find out how to balance readiness and your business' needs in this session.

11:45 - 12:25

Throwdown with Crowdstrike
Hear from a leading Crowdstrike expert about digital transformation.

Working on a Digital Transformation Framework — Discussing Core Components for Success and Catering for New Cyber Risk Exposures
Your organisation is probably undergoing digital transformation in some shape or form so it is imperative you're on top of the increased level of risk these bring with them. Join this session to hear how to balance new technologies and cybersecurity.

12:40 - 13:20

Fireside Chat: "Instead of thinking out the box, get rid of the box" — Supply Chain and Third-Party Risks
Time to get the brain juices flowing and think out of the box about supply chain risk, up to now a problem few people have the answers to but one of the biggest facing the cybersecurity community.

13:35 - 13:55

Real-life Experience: Challenging the Cyber Risk Status Quo: Experiments with Quantitative Risk Analysis
Personal experience are key for cybersecurity professionals to learn from and in this session Cameron Prescott Young, Head of Security Management & Assurance, Legal & General, shares his personal experiences of trying to understand and adopt quantitative risk analysis methods for cyber risk.

14:10 - 14:40

Infosecurity Europe Hall of Fame Ceremony

14:55 - 15:15

Case Study: Roadmap for a Product Security PSIRT
Hear from Cannon Europe about how the company created the Product Security Incident Response Team (PSIRT) as part of a review of its information security. If you're curious about how to drive a security proposition based on a more secure product this session is for you.

TECHNOLOGY

15:30 - 16:10

Fireside Chat: IoT Devices and Big Data: A Boon and a Curse
IoT devices, we've probably all got a camera or a smart speaker in our homes but how safe are they? And is the regulation keeping up with the development of these devices? Find out more in this session about IoT at home and in the business environment.

16:25 - 17:05

Fireside Chat: Digging Deeper on Threat Hunting and Effective Incident Response, Innovative Deception Technologies for Proactive Cyberdefence Tactics — Implementing Guidelines
Ever thought about how to create decoys and turn the tables on the attackers? This session will teach you how to add cyber deception tools to your security stack, and importantly how to maintain them.

THURSDAY 22 JUNE 2023 DAY THREE

CULTURE & SKILLS

11:05 - 11:45

Throwdown: Neurodiversity in Cyber — Why It's a Competitive Advantage
Hear about the benefits of hiring neurodiverse talent in cybersecurity and how to approach this with a talent management strategy.

The Achilles' Heel of Cybersecurity Industry — Cyber Talent Management and Focusing on the Human Deal
Everyone knows cybersecurity is facing a skills challenge. We need to optimise human potential and this session's speakers will deliver inspirational thought-leadership on how to tackle the challenge.

12:00 - 12:20

Cybersecurity As a Technology Lifecycle Issue: Why True Resilience Demands a New Operating Model
This session will help you understand the true advantages of an end-to-end approach to cybersecurity and offer practical advice for businesses that want to future-proof their strategies.

12:35 - 13:15

"Culture eats strategy for breakfast" Building a Strong Culture of Cybersecurity Awareness — Embedding Security as an Ideology in the Enterprise
Designing a human-centric cybersecurity programme is key to success but it is by no means an easy task. Join this session to be inspired and learn how to overcome barriers to creating a positive security culture.

13:30 - 14:10

Ignore Burnout at Your Peril — Mental Health and Insider Risk as the Next Big Threat to Cybersecurity
In this session we'll be trying to answer questions like: If stress and fatigue are becoming the norm, what should stakeholders be doing to ensure the resilience of the cybersecurity team is not compromised?

EMERGING THREATS AND FUTURE TRENDS

14:45 - 15:05 What Does our Hyper Connected World Have in Store for You and How Can You Devise an Insurance Plan?
Preparing for the future is critical for cybersecurity professionals. This session take a deep dive into the complex dangers and how you can start building protections against them.

EVENT AT A GLANCE

There's so much going on at Infosecurity Europe….here are my top things to check out at this year's event.

Time for some fun

The Gaming Zone
Get ready to unlock your playful side and embrace old-school fun in the Gaming Zone! Presented in partnership with TikTok, this is the ultimate opportunity to flex your competitive muscles, test your skills, and relive classic gaming moments. Why not take a break from your day and level up your enjoyment with some retro gaming action?

Cyber House Party
Fancy dancing the night away? Head to the Cyber House Party (CHP) after-party with live DJs on Wednesday evening, 21 June 2023. The event will bring together the cybersecurity community in aid of NSPCC Childline. CPH can't wait to see you all there. Watch this space for more info. www.cyberhouseparty.com

Happy Hour

Exhibitors will be hosting 'happy hours' on Wednesday 21 June, 3.30pm - 5.30pm, to bring everyone together for free drinks and free-flowing conversation on their stands. Check out who is hosting one in our Exhibitor A-Z. A unique networking opportunity and time to enjoy our exhibitor's hospitality.

Champagne CISO*
Club CISO will be hosting an exclusive networking event Wednesday 21 June at 3pm. This interactive session will inform, educate and most importantly entertain. ClubCISO will inform attendees of trends in the cybersecurity sector that have been observed over the past 12 months. In this open discussion, no views will be attributed to individuals or organisations.

*This session is only open to Leaders' Network badge holders.

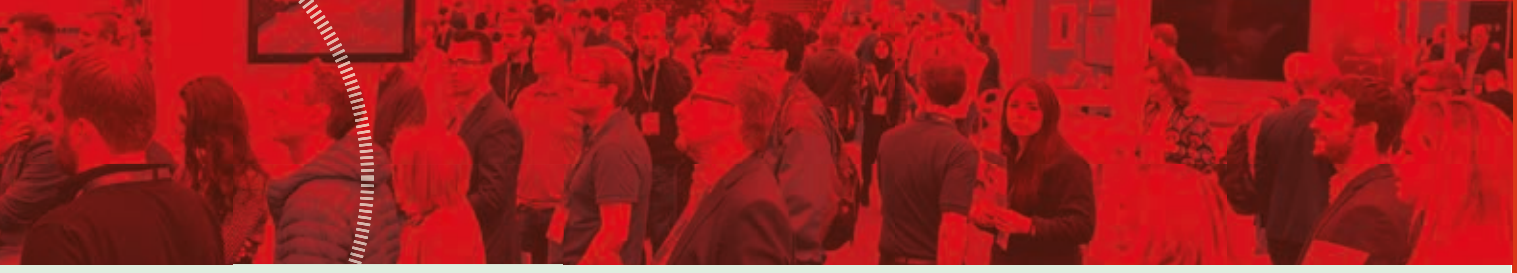
Essential Learning

Hack The Box @ Geek Street
Hack The Box is back for the second year of our Geek Street feature. Here, you can put your security skills to the test and participate in an exclusive 3-days Live Hacking Competition and Workshop. Various hacking challenges await you, carefully designed to demonstrate the latest attack techniques and vectors in web, cloud, forensics, and more. Anyone can join the Hack The Box squad and test their security skills.

Security Workshops
Benefit from in-depth, practical sessions offering advice on how to strengthen your information security posture. The workshops range from 90-minute training sessions to tasters for industry certification programmes with a range of formats group work, panels and presentations. Develop your skills while networking with your peers.

Conference Programme
The Infosecurity Europe Conference programme offers a unique opportunity to learn from industry-leading speakers about real-life security challenges and how to overcome them. The programme features a variety of session formats including one-to-one interviews, panel discussions, presentations and attendees have the opportunity to earn CPE credits in much of the sessions. More information on the conference programme can be found on the Infosecurity Europe website.

SCAN ME TO DISCOVER THE FULL CONFERENCE PROGRAMME



Leaders' Programme

Open to CISOs and Head's of Information Security the leaders' programme ensures your visit to Infosecurity Europe makes the most of your limited time. To join the programme simply register for Infosecurity Europe where you'll be prompted to join the programme.

Leaders' Programme highlights

- Access to the exclusive Leaders Lounge away from the show floor, located in the South Gallery Rooms.
- Exchange knowledge with those in similar roles across varied sectors.
- Opportunity to invite one guest to Infosecurity Leaders Lounge (guests must be accompanied at all times by their host).
- Participate in the Leader's Roundtables hosted by Netskope (Day 1), F5 (Day 2), and Armis (Day 3).

Explore Innovation

Start-up Showcase
The start-up showcase is reserved for recent companies with start-up status. Featuring bite-size presentations, discover the newest tools being developed to protect against the latest threats. A must-attend stage for Infosecurity professionals that want to stay ahead of the curve.

DSIT Innovation Competition
For the eighth year running, the Department of Science Innovation and Technology (DSIT) has been looking for the most creative and original cybersecurity companies in the country, one of which will be crowned The UK's Most Innovative Cyber SME 2023 at Infosecurity Europe. TryHackMe was crowned the winner at the event in 2022 and joined an impressive list of past winners including CAPSLOCK (2021) and Hack the Box (2019). This is a must-see for those wanting to inform themselves on cutting-edge innovations in cybersecurity.

Discovery Zone
The discovery zone is reserved for exhibitors and vendors new to Infosecurity Europe. It brings together established companies and start-ups at the forefront of innovation, delivering cutting-edge technology and solutions, making this area a must-visit for information and cybersecurity professionals looking for the next big thing.

Infosecurity Magazine Events

Women in Cybersecurity
Sponsor: CROWDSTRIKE

Infosecurity Magazine is excited to be hosting the seventh annual Women in Cybersecurity networking event at Infosecurity Europe on Wednesday 21 June, 2023, at 11.30am. Featuring a keynote presentation by Danni Brooke, former undercover police officer and now Hunter on Channel 4's hit show, Hunted, this exclusive event will also include a networking lunch and a panel discussion featuring some of the industry's most inspiring women.

Executive Briefing
Sponsor: expel

An *Infosecurity* Magazine executive briefing will be taking place at the start of the day on Thursday 22 June, allowing you the time to grab a coffee and a chat beforehand. The briefing will focus on specific security challenges and offer you an opportunity to discuss solutions with peers. More details coming soon.

Meet the Team
Visit the Infosecurity Magazine stand L90 to chat to the team, pick up a copy of the latest magazine and get a free Cyber Hygiene Checklist.

What You Need Before You Go
Download our official app to plan your day, pre-book meetings, keep track of the conference sessions you're interested in, find your way around the show-floor and connect with companies you would like to meet.

Remember – no badge means no entry to Infosecurity Europe. So, make sure you've got your badge printed out in advance, ready to go for the event. If you have any further questions about show safety or visa requirements, we've compiled a list of FAQs for you to give you the answers you need: https://www.infosecurityeurope.com/en-gb/help/faqs.html

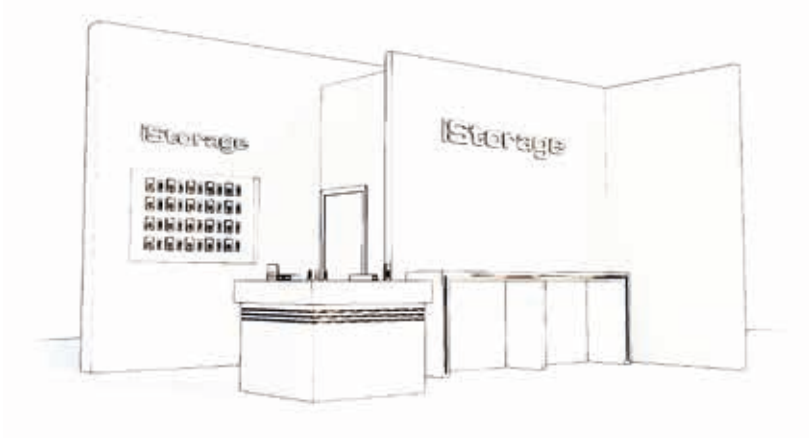
iStorage®

PIN authenticated, hardware encrypted,
data storage & cloud encryption devices.

Be the first to see our **new product**!

- **New product!**
- **Free product giveaways***
- **Daily prize draw/competition**
- **Special show pricing**

Come and visit us on stand **S70**



First 10 visitors** to show us this advert on our stand will receive a datAshur PRO 64GB encrypted USB flash drive for **FREE!

FIPS 140-2 Level 2/3

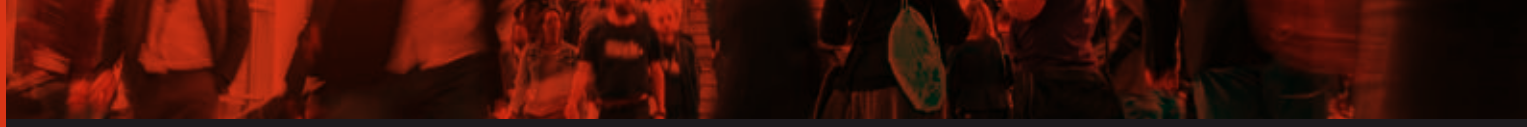
Commercial Product Assurance (CPA)

Baseline Security Product Assessment (BSPA)

NATO Restricted Level

iStorage®

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



EXHIBITION HIGHLIGHTS

Infosecurity Europe brings together leading vendors and service providers to showcase the latest technologies and solutions. There's no better opportunity to see innovation first-hand, test and benchmark solutions, build valuable relationships and make properly informed product choices that ensure ROI.

Here is a snapshot of what some of the exhibitors will be sharing at this year's event.

Create a Personalized Threat Intel Report with CrowdStrike

Attendees will be able to generate their own personalised threat intel reports with CrowdStrike at the company's stand X20, developing an adversary insight analysis based on their region and industry.

CrowdStrike will also be demonstrating all its solutions, with identity and cloud key topic areas for 2023, and have risk review offerings for both Cloud and IDP solutions.

In addition, CrowdStrike will be leading the Women in Cybersecurity session to be hosted on Wednesday June 21 from 8.30-11.00am.

Hear from Hornetsecurity at the Technology Showcase

On Tuesday 20 and Wednesday 21, Hornetsecurity will be sharing two topical presentations at the Technology Showcase.

At 16.40 on June 20, learn about the latest threats and how to protect your business effectively by listening to the talk titled "Today's Evolving M365 Threats and How to Mitigate Them." Mitigations and considerations from yesterday may not be enough in today's threat landscape. Matthew Frye, Head of Presales and Education at Hornetsecurity, will help you understand if your Microsoft 365 tenant is ready to weather the storm.

On June 21 at 16.00, Hornetsecurity will be diving into AI with their presentation titled "ChatGPT and AI: Armageddon for the Cybersecurity Industry?" There are some schools of thought that say the increase in AI usage may spell disaster for cybersecurity teams. Is this really the case though? Andy Syrewicze, Security Evangelist with Hornetsecurity, will attempt to answer some of these questions for you. You can also speak to the Hornetsecurity team at stand N40.

Understand How to Survive a Breach with Illumio

High-profile breaches continue to dominate the headlines, and companies need to shift the focus from preventing attacks, to surviving them. Illumio's CTO, PJ Kirner and Bishop Fox, the leaders in offensive security testing and adversarial emulation, will present a Strategy Talk at 11:30 on Thursday June 22 on why every pound spent must have a measurable impact towards resilience.

Located on Stand S40, Illumio and its partners will also present a series of live demonstrations on how companies can use Zero Trust Segmentation to build cyber resilience, including ransomware containment.

Additionally, the company will be showcasing a series of new innovations including: Illumio for Azure Firewall; Illumio's new Incident Response Partner Program; and new dashboards to help customers better protect themselves against ransomware.

Meet the threatYeti with AlphaMountain

AlphaMountain will be featuring the threatYeti product at Infosecurity Europe.

threatYeti is a domain research platform for cyber threat analysts of all skill levels. The product also protects cyber threat analysts and their networks from risky sites.

threatYeti's no-click categorisation presents sites into at least one out of 83 categories so that analysts don't have to visit them and risk encountering objectionable material or downloading malware. With threatYeti, AlphaMountain is making domain threat intelligence a core competency inside organisations of all sizes. Get a demo of threatYeti at booth U45.

Learn About Digital Trust with DigiCert

Understand how digital trust secures a hyperconnected world with Rich Hall, AVP, technical sales with DigiCert, who will be speaking at the Insight Stage at 13.30 on Thursday June 22.

Digital trust as a strategic initiative reduces risk of business disruption, reduces attack surfaces, improves crypto agility and drives business innovation. In a world that is becoming hyperconnected, digital trust is the essential glue that bridges security and identity.

Join this session to learn how companies can achieve fast time to value with their digital trust initiatives, for diverse use cases ranging from protecting enterprise users and systems to securing medical devices, building trust in election outcomes and more. Visit the DigiCert team at stand E40.

Find Out if Your Organisation is Susceptible to HEAT attacks with Menlo Security

At Menlo Security's Tiki-themed stand AA60, visitors can learn more about Highly Evasive Adaptive Threats (HEAT) and find out if their organisation is susceptible to HEAT attacks through the company's HEAT Check penetration tool. Visitors are welcome to sign up for HEAT Checks and demos at: https://calendly.com/menlo-security/infosecurity-europe-june-2023

Menlo Security will also be hosting customers, prospects and partners at the Fox Pub (outside the ExCel) from 11am-11pm on Tuesday 20 and Wednesday 21 June where the company will be offering food and refreshments. To register, visit: https://info.menlosecurity.com/Menlo-Security-Social-InfoSec-2023.html.

Join Invicti for Coffee with Zero Noise

Cybersecurity is loud. Endless jargon, acronyms, and tools – it's noisy, but Invictus aims to deliver AppSec with Zero Noise.

Head to their booth L20 for a coffee from their zero-noise coffee machine and even enjoy a specialty Invicti drink.

Zero noise means the most accurate, efficient and evidence based AppSec. Continuous application security with zero noise is designed to be reliable for security, practical for development and serve critical compliance requirements.

Invicti director of product management, Jonny Stewart, will be speaking on June 20 on "2023 Vulnerability Trends: A Deep Dive to Improve AppSec Programs" at the Insight Stage between 13.30-14.15.

Get Interactive with DigitalXRAID

Centred around the theme 'don't let the bad guys win,' DigitalXRAID will be running a range of interactive activities and live demos on its stand M50, with experts on hand to answer questions attendees have about their own security posture and roadmap.

DigitalXRAID is also running a gamified workshop to test guest attendees and industry experts on their approach to risk management. The workshop will cover topics front-of-mind for business and security leaders, including how to get buy-in from the board for security programmes and how a proactive strategy can reduce business costs and deliver ROI.

Meet Lead Security Analyst, and CREST International Council member, Alan Freeland, at the stand to get advice, answers to questions and assistance in DigitalXRAID's open surgeries throughout Infosecurity Europe.

Join Semperis' Leading Security Experts for Real-Life Stories

Microsoft's Active Directory has become a prime target for cyber-criminals. Semperis is inviting Infosecurity visitors to stand E62 to hear about the risks from two leading security experts:

The CISO's take on identity-first security: a Q&A with Simon Hodgkinson, former CISO at BP and Semperis strategic advisor, on how to boost operational resiliency and stay ahead of identity-based cyber-attacks. These sessions will take place on June 20 from 10.00-10.30 and June 21 from 14.00-14.30.

War stories from the trenches: Senior Incident Response Lead Jorge de Almeida Pinto, Semperis, shares real-life stories around how he has helped organisations stop potentially business-crippling in-progress identity system attacks. These insights will be held on Tuesday 20 June at 11.00-11.30 and Wednesday 21 June at 15.00-15.30.

Discover What a Passwordless Future Will Look Like with LastPass

Data shows that 80% of data breaches are the result of compromised login credentials. These are credentials, like shared accounts or un-managed apps, that traditional Identity tools – SSO, MFA, PAM – simply don't secure.

The natural solution? Go passwordless. Password managers have been on a mission to reduce reliance on passwords for well over a decade, and now they are the key to transitioning to passwordless quickly, securely and easily.

As an industry leader in passwordless access, LastPass will eventually remove the master password altogether, delivering on the promise to reduce user friction while simultaneously enhancing security.
Visit stand M95 to learn more about how LastPass can help prepare you for going passwordless in the future.

Discuss the Email Security Landscape with Egress

In recent years, phishing attacks have become increasingly prevalent and sophisticated; in fact, 92% of organisations fell victim to successful phishing attacks in the last 12 months, while 91% of organisations admit they have experienced email data loss.

Meet the Egress' team of experts at booth P50, who will provide in-depth personalized demonstrations of its Integrated Cloud Email Security platform that prevents advanced phishing attacks and outbound data loss.

Attendees are also invited to connect with Egress' VP of Threat Intelligence, Jack Chapman, before and after his session taking place from 12.15-12.40 Tuesday, June 20, where he will discuss whether AI opens a backdoor to your organisation that attackers can use.

Additionally, Egress will be giving away bound copies of its recent Email Security Risk Report.

Gain Pentesting Insights from Pentera

Visit stand W40 to hear about the latest trends and best practices in pentesting from Pentera experts. The firm will also provide insights on its newly published report surveying 300 CISOs from enterprises with 1000+ employees across the USA and Europe, focusing on their overall security and security validation practices, how they are managing exposure, and the differences in the markets.

Get Involved in the Information Sharing and Analysis Center

The Information Sharing and Analysis Center (ISAC) is encouraging security pros to visit stand F34 to learn more about how their organization can get involved with the non-profit organization.

Nearly a dozen ISACs members will be at the show, representing industries including retail and hospitality, aviation, health, financial services and automotive. Throughout the event, presentations will be given on how ISACs facilitate collaborative sharing environments that strengthen cybersecurity teams.

WHO'S EXHIBITING

KEY
Discovery Zone - DZ
Start-up - SUp
US Pavilion - US
Happy Hour -


Infosecurity Europe
20 - 22 June 2023, ExCeL London
Join us
as we rethink the power of infosecurity
Keep up to date on the latest advances and innovations
Connect with the brightest minds
Get hands-on with the technology
Benchmark your solutions and strategies
Register at www.infosecurityeurope.com

NETAND: A company that connects people and networks

Ho Chul Shin, CEO, NETAND

As business processes continue to be digitized rapidly, IT environments are becoming more distributed and dynamic with each passing day. With growing IT infrastructure, security risks—ransomware, malware attacks—are also spiraling at an unprecedented rate. Even small security challenges can cause major disruption, undermining the reliability of the organization involved and endangering customer data. Along with ongoing digital transformation and the proliferation of cloud, that dispersal introduces new challenges for the cybersecurity community.

In addition to the rapid changes in the security market, digital security continues to pose many risks. Another prominent loophole, especially for cyber-criminals, is identity theft and unauthorized access. This cyber theft is often attributed to legacy security protocols in organizations that still rely heavily on manual processes. Insider threats pose a major risk to the organization because they include insider knowledge of an organization's resources, such as facilities, IT equipment, network information, and computer systems, and people with access to them.

The Genesis of HIWARE Solution

NETAND has been delivering innovative network security solutions since its inception in 2007 to ease these customer concerns and deliver value beyond the network and to help efficient systems management and protect organizations' complex IT infrastructures.

Despite the constant changes in the IT environment, NETAND has continued research and development of integrated IT operations management solutions and extensive experience with diverse customers. Our flagship solution, HIWARE, focuses on addressing the most pressing cybersecurity challenges, including zero trust, ransomware, vendor and employee remote access, cloud security, compliance, and cyber insurance requirements.

HIWARE even works with major CSPs as well as on-premises to integrate and manage resources that are dynamically changed and allocated in the cloud environment through API linkage and to improve security management efficiency by reflecting resource changes such as number of virtual equipment and IP addresses in real time.

It has established the standard for integrated access and account management solutions with industry-leading technology and expertise and has established itself as a leading company in the South Korea market. Users can safely operate and manage system access control, account management, and password management within a single platform and framework.

Next Gen Integrated Identity and Access Management

HIWARE Identity Management (IM) solution features an automated and integrated approach to managing all user accounts scattered across systems (on-premises or cloud). This enables the IM solution to sync and consolidate all identity types in real-time, without lags in status updates that cyber attackers are always ready to pounce on and it also automates the account and password management process to increase efficiency.

The hassle with identity management is incorporating it with the various systems and digital infrastructures that clients have in place and even from a technical aspect, it is important to incorporate an IM solution with other solutions which may cause usability problems. However, HIWARE is configured to incorporate the IM solution while maintaining the various processes of its clients as much as possible.

NETAND also provides Privileged Access Session Management (PAM) solution which enables end-to-end management and supervision of users by controlling all accesses and operations of clients' IT infrastructure such as networks and servers, monitoring work details in real-time, and saving log records. "We not only provide identity management solution but also deliver access management solutions in one single UI to eliminate security concerns of our clients," states Shin.

Additionally, HIWARE renders IM and PAM solutions for clients' DBMS. The solution collects the clients' accounts scattered across DBMS and automatically manages account life cycles and passwords, from the point of creation to deletion, in accordance with clients' security management policies.

It's unified and automated identity management features streamline clients' DBMS accounts management, allowing them to save time and costs significantly. On the other hand, our PAM for DBMS grants access to personal information databases and provides authorization data separately to each user to prevent leaks of personal information and confidential documents.

"Our solutions provide impenetrable security to clients' systems while supporting an unlimited number of devices and users without any lag or downtime, even if we don't get a request, we keep analyzing how our clients' system works with our solution," adds Shin. This upfront approach has enabled NETAND to achieve up to 65% share of the identity management market which global vendors in South Korea majorly occupy.

Build Your Own Solutions

The whole tech industry is dynamic and constantly changing. And if you're in IT security, you're in a unique position that the changes can be forced upon you by techniques developed by malicious hackers and faster than other industries. That means that there's always something new going on in the industry.

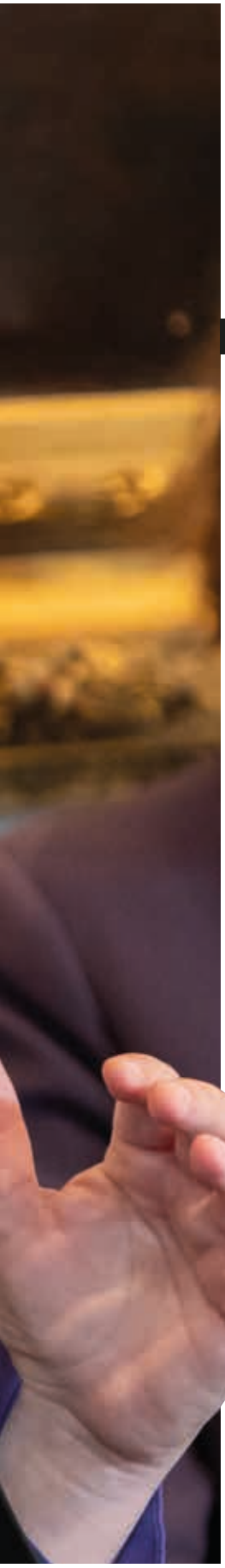
In this dynamic environment, organizations must maintain the security of their corporate infrastructure and assets, including data. At the same time, organizations need to provide the right level of access to all users in a smoother and more efficient way to perform tasks.

NETAND's HIWARE helps organizations simplify and automate account and access control management tasks and enable more granular access controls and permissions. With our solution, the IT team no longer has to manually assign access control, monitor and update permissions, or disable account provisioning.

NETAND is the first integrated access and account authority management solution in Korea that applies artificial intelligence (AI) technology. Real-time analysis of user history data can detect even intelligent illegal activities that are not detected by policies. This AI-based deep learning technology is a next-generation solution that periodically automatically analyzes and updates user patterns to improve security on its own like a living organism.

Despite the ever-increasing reliance on IT infrastructure and the complex and diverse threats of information security and incidents, enterprise security management can be simplified.

NETAND



In childhood Sian John was described as a polymath, 25 years into her career as a cybersecurity professional this remains the perfect characterization. *James Coker* meets Sian to find out about her unique skillsets and journey in the sector, which culminated in the award of an MBE in 2018

SIAN JOHN

Sian John's mother's description of her daughter as a "polymath" in childhood provides further credence to the well-worn phrase 'a mother knows best.' From speaking to Sian, it is clear that this label remains just as relevant today, having enjoyed a 25-year career in cybersecurity and counting.

From history and classics to science and, of course, computing, Sian has thrown herself into new challenges throughout her life without hesitation. Even while working in senior cybersecurity positions, she completed a BA in Humanities in Classical Studies in 2012 before an MA in the same subject in 2018.

Sian has also been learning Latin for a number of years and has ambitions to complete a PhD in Classics once she has retired from working life.

Her love of Classics has kept her firmly on European soil throughout her career rather than crossing the pond to the US. "I've had offers and I'm always like 'you haven't got any Romans over there," she laughs, reflecting on her love of walking around ancient Roman cities like Pompeii and Herculaneum for holidays.

This passion is only exceeded by her desire to strengthen society's cybersecurity in the UK and beyond. In addition to her current role at Microsoft as senior director of the tech giant's security business development, Sian devotes much of her time to her prominent positions at non-profit and government-backed cyber organizations, including UK Research and Innovation (UKRI), the national funding agency investing in science and research in the UK, and trade association TechUK.

Her commitment to the cybersecurity cause is demonstrated by the hours she puts in. Sian explains that in her current post at Microsoft she works US hours on a few days of the week, "which means that I often do the TechUK and advisory work in the morning."

She adds: "It's very important to me that Microsoft doesn't suffer because I do it – although my boss is very supportive."

It was her extensive and highly impressive work in the field that led to Sian being recognized with a Member of the Order of the British Empire (MBE) award for services to cybersecurity in 2018. However, Sian briefly hesitated accepting due to its association with the British Empire, which she says "I'm not a massive fan of." Nevertheless, it was a huge honor, and Sian admits to feeling stunned when she was informed of the award.

"I never expected it – I'm not the sort of person to get that kind of recognition," she says modestly.

> ***"I worked out how to put a password on it; my first security task was as simple as that"***

This sentiment is very much in-keeping with Sian's personality – grounded and focused on making a practical impact rather than personal gain. However, she is delighted that prominent individuals in the sector are being increasingly recognized for their work, also citing the MBE awarded to Nicola Whiting in 2020.

A Polymath Child

Sian's passion for computing, and ultimately, cybersecurity, dates back to her childhood years in the late 1970s and early 80s in Yorkshire, England, where she grew up after being born in Wales. "I was quite a techy, geeky kid," she grins.

Her father, a maths lecturer educating primary school teachers, used a computer to prepare lectures, which Sian was able to take full advantage of. "I went to college with him and he had a ZX81 computer, so I played around with that," she recalls.

Sian also had access to a BBC Micro Model B computer her father brought home, working out how to set up games by herself. "My brother is five years older than me but he didn't understand the computer so I had to load the games and then he'd come and beat me at them," she laughs.

Additionally, Sian attended a summer school class her father organized for 10-year-olds that involved the use of computers, but was the only girl in the room. "I was always a bit overwhelmed but I heard later on that I was the best in the room – I didn't feel like that because the boys kept telling me that I wasn't."

It is a mark of Sian's mindset that she wasn't put off by others – pursuing new skills and passions regardless of the situation. It is a trait that continues to serve her well today.

As alluded to, computing was one of many hobbies for Sian growing up. Having developed an early interest in physics, she was a member of the British Association of Young Scientists and an avid reader of sci-fi books.

Additionally, she was an active participant in the Air Cadets, continuing until the age of 21, attaining the rank of Cadet Warrant Officer. If all that wasn't enough, Sian was a member of a music band.

The downside to Sian's polymath tendency was that her A-Level studies suffered as a result. "I did Physics, German and Maths but I didn't work hard at those because I had Air Cadet meetings twice a week, band practice on a Wednesday night and then on weekends there'd usually be a Church fete or something which we'd play at," she explains.

Does Sian regret not putting enough time into her academic studies at that time? Absolutely not, as it ultimately led to her pursuing a career in cybersecurity. →

"I don't regret it because I wouldn't have gone the direction I did," she notes, adding: "The best thing I did was be in the Air Cadets and not do much in my lower sixth."

Computing Her Interest

Unable to get red brick university place following A Levels, Sian then attended the Nene College of Higher Education, now the University of Northampton, studying a Bsc (Hons) in economics, computing and business from 1989-1992. These were all topics of interest to Sian and at the time "I either wanted to be an economist or work in IT."

The computing aspect was mostly based around systems analysis and design, with security not really an aspect.

Ironically, the decision to pursue a career in computing was confirmed just after being accepted on a Master's course to study Economics at the University of York. Between finishing her undergraduate degree and starting the MSc course, Sian was offered the chance to do what she described as "casual IT work" at the college where her dad worked. This initially involved building a couple of IT systems, including a computerized learning system.

This soon led to further opportunities, such as implementing a room booking system and migrating registry systems. Importantly, this enabled Sian to learn "how to talk about IT to others." As her work at the college grew, Sian was required to attend meetings at the registrar, where she'd essentially have to act as "translator" for her colleague who "spoke in the language of Unix."

Securing Democracy

It was work that she quickly fell in love with, and after completing the MSc in Economics, Sian soon landed a role at the Houses of Parliament in 1995, initially as IT Manager in the Serjeant at Arms Department.

An interesting and, at times, eye-opening experience, it gave Sian her first taste of cybersecurity, and she never looked back. This first cybersecurity task related to a salary app that had been written into the Parliamentary IT system, which, while out of date, was accessed by an employee. "So I worked out how to put a password on it; my first security task was as simple as that," recalls Sian.

> ***"I want to make the world a better place and make a difference and that is the Microsoft culture"***

Suspecting that other sensitive information was similarly exposed, Sian explains that she went around all the other departments of Parliament, such as finance, to find " their sensitive bits and put a password on them."

Looking back, it is astonishing to think that one of the oldest and most significant institutions in the world failed to have so much as a password to protect sensitive files – in reality, this neglect was a symptom of its times, with few considering cybersecurity issues.

From there, Sian became Systems Engineer at the Parliamentary Communications Directorate, where security finally became a significant issue to the UK's home of democracy. "I went there to develop new systems but I pretty much took on looking after the firewalls, working on mail and web security, putting proxies in place," she notes.

This experience cemented Sian's desire to pursue a career in cybersecurity. She says: "I realized I don't just want to build stuff, I want to make it secure and protect it against people – there's no point building it if anyone can get into it."

Yet, at that stage Sian still wasn't described as a security professional – rather a generic IT worker. Cyber simply wasn't seen as a standalone career at this stage. And her next position after the Houses of Parliament was a non-security role as a Project Executive at Reuters – something she quickly moved on from.

A Cyber Focus

Eight months later, and Sian took her first cybersecurity focused role – joining security vendor Ubizen, later becoming Cybertrust, as a senior/principal consultant. This is a job she immediately loved, consulting with customers and finding solutions to meet their needs.

Undertaking a wide range of tasks helped keep the job interesting for Sian. "One week I'd be building someone's firewall then the next I would be writing their security strategy," she explains.

This work also exposed Sian to pen testing, and she particularly enjoyed 'blue teaming' – hardening systems to repel attacks. She recalls a competitive pen test on a customers' system where she and colleagues raced each other to hack into their system. After one of her colleagues found a way in very quickly, "I hopped on the box and started hardening it to stop others getting in," says Sian.

While she admits it would take her longer than her colleagues to hack in, Sian was particularly good at hardening network defenses once vulnerabilities were discovered. "This has always been where my interest has been – how we make it better," she explains.

After six years at Cybertrust, Sian decided she was ready for a new challenge, joining another cyber focused company in Sygate, which was about to be acquired by Symantec. This was in a sales and consultancy based position, which required periods away staying in different locations across the UK.

It was this experience of frequently staying in hotels and travelling that led to Sian's decision to indulge her passion for Classics, taking a BA in Classical studies at the Open University. This began in 2000 while working consultancy at Ubizen and continued into her role Symantec. "I was sitting in a hotel in Dudley [Midlands, UK], three months on site, and thought I need

something to do that isn't sitting in a bar reading a book. On my own I can be quite unfocused," she admits.

It is indicative of Sian's character that she wants to stay challenged and keep busy at all times – inside and outside of work.

Sian completed her BA in Classical Studies in 2012, achieving a first, before completing her Master's in the subject a few years later in 2021, starting in 2018. She reflects that had her school life gone differently, with a better History teacher, she may have instead sought a career as a historian, likely focusing on Ancient Rome.

"It's probably worked out well," she laughs.

In total, Sian spent nearly 12 years at Symantec, moving from a sales-based role to more strategic, business-level thinking, which also involved increasing speaking and media engagements. This was first as director of security strategy at Symantec's UK and Ireland Enterprise and then becoming chief strategist, EMEA.

A New Challenge

It was the perfect grounding for Sian to take the next step in her career, at tech giant Microsoft in 2017, which was in the midst of a major expansion in the cybersecurity market. Much of her previous roles involved helping clients secure their Microsoft systems, therefore "I thought actually going to the platform would be interesting."

Despite working in pure play cybersecurity companies for many years, Sian admits to being blown away by the security culture within Microsoft, spearheaded by current Chairman and CEO Satya Nadella.

"Security is absolutely core to the culture of Microsoft, making sure everyone treats customer data responsibly, works responsibility and engages with technology well," she explains. "I want to make the world a better place and make a difference and that is the Microsoft culture."

Following several advisory positions, Sian became senior director of Microsoft's security business development in November 2020, which she acknowledges is outside of her comfort zone. Her team analyzes the wider cybersecurity market, identifying developing areas and organic growth opportunities before developing a business case to the CEO and CFO for investment.

> ***"I just want to feel like I'm making a difference, whether it's to people that work for me or to the industry"***

While Sian has found her previous studies in economics and business have helped, "I learn every day from my team because they are business development people and I'm a cyber person in business development."

In keeping with her whole life, Sian has never been shy of accepting a challenge and learning new skills. "It's really interesting to take that step back from the technical and think about how Microsoft grows its business," she comments.

While business development planning was not an area Sian was accustomed to prior to taking her current role, her extracurricular work at trade association TechUK as chair of its Cyber Management Committee and council member of the UKRI's Engineering and Physical Sciences Research Council (EPSRC), helps as it gives her a more holistic perspective of the cybersecurity industry.

"It's actually very complimentary to my job in terms of thinking where the market's going and what we need to do," she explains.

This includes enabling Sian to get first-hand insights and involvement in the ambitious UK government-backed Digital Security by Design (DSbD) project, which aims to create technologies capable of securing underlying computer hardware.

In addition, she is heavily involved in the government's Cyber Runway program, which assists innovative cyber startup firms launching and growing their company and solutions. "In the job I'm in, knowing the startup community is very useful, so I'm very engaged," she says.

Future Plans

While Sian has raised the prospect of retirement in the next decade, albeit to complete a PhD in Classics, there is still plenty more she wants to contribute towards in cybersecurity, despite never having had a formal career plan.

Sian also notes the next five to 10 years are likely to be especially exciting for the development of the cyber industry. This is because security is now being seen as an important business issue in the boardroom, while the development of technologies like AI and quantum are set to transform cyber-attacks and defense. These are changes Sian very much wants to be part of.

"For me professionally, I just want to feel like I'm making a difference, whether it's to people that work for me or to the industry," she outlines.

As the years go on, Sian has become increasingly determined to help guide and mentor the next generation of cyber professionals.

"In the past 10 years in particular, I have flipped from it's about my success to the success of those around me – that really motivates me," Sian outlines.

This includes encouraging more women into the industry, "but actually anyone who's young and passionate, I want to help them be successful," she adds.

Given her track record, it's in all of our interests for Sian to stay in the cybersecurity industry for many more years to come – despite the lure of classics, I suspect that will be the case

SECURING THE SUPPLY

Kate O'Flaherty investigates what organizations have learned three years on from the SolarWinds attack and what more needs to be done to overcome today's supply chain security challenges


CHAIN

It's a stark and frightening reality that a single security weakness in the supply chain can provide criminals with access to a whole network of interconnected organizations. Take the example of SolarWinds, the 2020 cyber-attack that sent shockwaves through the business world after adversaries infiltrated companies and government agencies via a malicious software update. And who could forget the Log4j vulnerability, which is still causing problems after demonstrating the weaknesses inherent in the software supply chain.

Three years after SolarWinds, organizations including the UK's National Cyber Security Centre (NCSC) and US Cybersecurity and Infrastructure Security Agency (CISA) continue to warn of the risks posed by the supply chain.

In 2022, the NCSC highlighted figures from the DCMS' *Cyber Security Breaches Survey 2022* that showed only one in 10 businesses review the risks posed by their immediate suppliers (13%). Worryingly, the proportion for the wider supply chain is even less (7%).

The risks to businesses are so grave that CISA has published a three part series on securing the software supply chain. Developed in collaboration with the National Security Agency (NSA) and the Office of the Director of National Intelligence (ODNI), the series provides recommended practices for customers to ensure the integrity and security of software during the procuring and deployment process.

However, supply chain attacks continue to plague businesses. Over the past year, Uber, GitHub, Magento vendor FishPig and VoIP software firm 3CX have all suffered supply chain-related cyber-attacks.

In an increasingly digital world, organizations are often connected to hundreds of suppliers and vendors. "This expansive network makes it a herculean task to track the movement of data and identify all the entry points along the entire chain that could be vulnerable to attack," says Rik Ferguson, VP of security intelligence at Forescout.

It's also difficult to assess the individual security protocols of third-party vendors – something attackers are quick to take advantage of.

Learning From the Past

While supply chain attacks are still happening, the SolarWinds breach was a wake-up call for many firms. First and foremost, it highlighted the significant vulnerabilities that can be present in the software supply chain, says Javvad Malik, lead security awareness advocate at KnowBe4.

Lessons learned include the importance of monitoring suppliers and vendors regularly; the need for multi-factor authentication and strong password policies; and to limit access to sensitive data, he says.

> ***"Many organizations have begun to look more deeply into the onboarding of third-party suppliers and implemented stricter processes"***

The breach has also led to a more collaborative approach when working with third party vendors, which Malik says is "crucial" in establishing and enhancing supply chain security.

SolarWinds itself has made several security improvements since the attack, including a secure by design approach to product development. The firm hired former CISA chief Chris Krebs and Stanford University professor and ex-Facebook chief security officer Alex Stamos as consultants.

To make its supply chain more robust, SolarWinds also established a supplier security and privacy assurance Program and improved its supplier risk management process. Meanwhile, it has adopted a zero trust security model where users and devices must be verified before they can access data and applications.

The SolarWinds incident has highlighted the need for robust supply chain visibility and risk management, says Nigel Gibbons, associate director and senior advisor at NCC Group. He describes how the breach has resulted in more firms performing regular audits of supply chain partners.

"Companies have been implementing control frameworks to align compliance and ease auditing. People realize that threat intelligence and an incident response plan are critical, along with isolating affected systems, notifying stakeholders and collaborating with partners and industry peers when attacks take place," Gibbons tells *Infosecurity*.

The SolarWinds attack pushed lots of organizations – including Forescout – to reconsider and adjust internal processes to shore up supply chain security, says Ferguson. "Many organizations have begun to look more deeply into the onboarding of third-party suppliers and implemented stricter processes as a result."

The 2020 attack has seen firms acknowledge they need to take a more proactive and comprehensive approach, according to Dr Farshad Badie, vice-dean of the Faculty of Computer Science and Informatics at the Berlin School of Business and Innovation. "This includes implementing stronger vetting and auditing procedures for all participants in supply chains and implementing measures to detect and respond to attacks in real-time," he says.

High-profile supply chain attacks have forced organizations to stop relying on perimeter controls alone – which has been a driver in the move towards a zero trust approach, says Will North, chief security officer at HR software solution provider, MHR. However, he says organizations are still a long way away from having the right controls in place.

One big challenge can be understanding supply chains and the impact a vulnerability can have. "This can be particularly difficult from a software perspective, as one piece of software may have been built using many other third-party software and code," North points out. He cites the example of the Log4j vulnerability, which was estimated to have been used in 17,000 other pieces of software.

Securing Your Organization's Supply Chain

Change is starting to happen, but there is still a lot to be done to ensure supply chains are secure. This is especially key as digital transformation continues to accelerate post COVID-19. Supply chains are only going to become more complex and interconnected and over time, this will of course open more gaps for cyber-criminals to infiltrate businesses.

One trend likely to gain momentum is the use of supply chain attacks as a means to distribute ransomware, malware and other types of cyber threats, Malik says.

The rapid adoption of cloud-based services, the growth of the internet of things (IoT) and other emerging technologies will add new and unforeseen supply chain risks, he warns.

With this in mind, he outlines the importance of a "proactive, risk-based approach" to supply chain security "rather than merely reacting to threats once they occur."

Experts agree that supply chain security starts with procurement. All companies in the chain should be following the security basics such as timely patching to minimize the chances of being caught up in an attack.

When choosing a supplier, security needs to be at the core of the procurement process, says David Dunn, senior managing director, head of EMEA cyber security, FTI Consulting. "Think through the risk: define your core principles, make sure those are contractually agreed to and do your homework to ensure third parties meet your requirements."

Once onboarded, it's a good idea to inventory all vendors, says Dunn. "Make sure you have a clear process based on risk and criticality to monitor each vendor's external exposure. Re-assess your vendors' security controls to ensure they meet the strong cybersecurity and data privacy standards you defined at the outset."

If they don't meet the standards, Dunn advises removing the company from your suppliers. "Document everything along the way including data flows, and use technology tools to keep the process efficient, organized and repeatable."

While a holistic view is important, each individual in the supply chain has a part to play. Every company must focus on improving their own security processes to diminish supply chain risk, says Ferguson. As part of this, vendors should ensure each hardware and software product is accompanied by a Software Bill of Materials (SBOM), he says.

An SBOM contains a list of materials, libraries and components – including any vulnerabilities. "Organizations must require this information from suppliers," says Ferguson. "Without SBOMs, no firm can effectively assess the risks associated with every component or asset in its supply chain."

"Without SBOMs, no firm can effectively assess the risks associated with every component or asset in its supply chain"

At the same time, every element in the chain must be traceable from origin to completion. "This will ensure its integrity and consolidate nested trust in all components included," says Ferguson.

Well-defined agreements outlining data confidentiality, provenance and governance must be maintained among users, he adds.

Meanwhile, visibility is key. The NCSC offers a supply chain mapping tool to help firms work out their supply chain dependencies to better manage the risks.

While SolarWinds created some momentum for change, there is no quick fix that will ensure supply chain security. Instead, it requires a multifaceted approach, says Gibbons. As part of this, he believes organizations must acknowledge the threat and use it to build an effective cybersecurity strategy.

Practical steps include implementing more robust security controls and monitoring to detect and respond to supply chain attacks specific to an organization's own threat profile, says Gibbons. "It should lead to adoption of higher security standards and best practices, as well as better education of employees and supply chain partners via regular training and awareness programs."

Supply chain security may be complex, but companies shouldn't have to go it alone. As threats become more sophisticated, it's integral that governments and trade bodies play a role in supporting businesses. "They can provide guidance, share threat intelligence and promote best practices to address the threat landscape," Gibbons says END

How to Develop an Effective Patch Management Program

Zoë Rose

Regional and Supplier Information Security Lead, Canon Europe

Zoë Rose is a highly regarded hands-on cybersecurity specialist, with 10+ years experience working with teams around the world. Zoë is a Cisco Champion and certified Splunk Architect, who keynotes at international conferences.

@RoseSecOps

An ideal patch management program is a formalized approach to ensure solutions are maintained, with the appropriate persons aware of their roles and responsibilities. Sustaining patch levels helps reduce likelihood of incidents taking place and can even reduce their impact.

While it would be beneficial to have agreed approaches prior to deploying a solution, it's not feasible for organizations to start over.

Risk Appetite

The organization needs to define what it's comfortable with. For example, what is sufficient to be considered up to date to meet its needs, and what frequency of patches is required. Further questions to ask are does your organization need to align with any certifications and/or regulations? If yes, they may have their own frequency to align with.

To apply this to existing environments, it may make sense to create a more lenient requirements, and once the organization is aligned, further restrict the requirements until they meet the appropriate risk appetite.

Responsibility Matrix and Nurturing Awareness

Unfortunately, it is common for new solutions to be deployed without fully defining who's responsible for what aspect. Create a matrix that defines the maintenance of a solution, which would incorporate patching. This should include showing who takes over responsibility when someone leaves an organization.

Additionally, out-of-schedule patching for critical vulnerabilities can further disrupt individuals. This is why colleagues need to be made aware of the importance of collaboration to prevent unnecessary delays and frustration where possible.

Level of Criticality and Available Capabilities

Knowing the type of data and business criticality of a system or solution is key to helping you prioritize. It will also ensure you know how much testing is required, and what teams to notify when a potential outage takes place.

One challenge I see in organizations is the tooling or skills gap for solutions already in place. In that situation, a question to ask is this solution worth the cost if something happens, or would it be smarter to invest in a replacement?

Proactively Identifying Gaps

Consider how your organization stays aware of what solutions are in place, and the patch level deployed. Many organizations don't know what is in place or what's required in their environment. Restricting who can deploy solutions, creation of an authorized list and controls to track what's installed can greatly enhance your program. Patches may not always be deployed in a timely fashion and tooling can also assist in ensuring compliance.

Some patches require reboots, others may cause conflicts and the annoying ones may change default configurations. Testing environments or selecting sample groups from production, can validate a patch before full deployment.

Some solutions simply cannot be updated, but they are still required to be retained either temporarily or long term. As a result, responsibilities still exist and need to be documented, but a risk waiver may be applied.

Automation

It will not be possible to automate every aspect of patch management, but these technologies can enhance the program and reduce administrative overhead. This includes measuring patch levels, easily deploying patches en masse, restricting unapproved solutions and/or identifying vulnerabilities detected in solutions deployed END

Joseph Carson

Chief Security, Scientist, and Advisory CSO, Delinea

Joseph is an award-winning cybersecurity professional and ethical hacker with more than 25 years' experience in enterprise security specializing in blockchain, endpoint security, network security, application security and virtualization, access controls and privileged account management.

@joe_carson

Effective patch management is crucial to maintaining the security, stability and functionality of any IT infrastructure. However, under resourced security teams and the continuous proliferation of IT assets mean that businesses can struggle to maintain timely software updates across their network ecosystem, making them susceptible to critical threats like ransomware.

When planning your patch management strategy, the first step is to identify and include every element of your IT stack in the process. Effective patch management requires a quantified risk assessment so you know which data, applications and systems are critical to supporting your business. Not all patches are equal so you must ensure that those that increase the risks of your business are prioritized.

This means your operating systems, internal devices, applications and particularly web browsers, which are frequently targeted by cyber-criminals. All these components should be using, or running on, the latest versions. If you're only applying patches to particular applications and leaving other systems on legacy versions, it creates a disparity, which threat actors tend to thrive on.

It's also important to remember that some updates often require a system reboot to take effect. This is a crucial step that should not be overlooked, as it can leave your system vulnerable even after applying an update. Additionally, rebooting can help to clear cached data and potentially improve system performance. This means privileged access management is an important component, as it ensures you can access systems securely with credentials that can deploy patches. Once deployed successfully, the access can be deprovisioned. On-demand privileged access will significantly reduce your risk exposure as part of your patch process.

Most importantly, you should have a formal review and documentation process that makes patch management an ongoing business function, rather than a secondary responsibility of the security teams. Whenever a new update comes through, the security team should assess the patch, testing results and potential endpoints before deciding on deployment. The state of the system should be clearly documented before and after each patch application to facilitate troubleshooting in case of future issues.

Updating software is only one aspect of a comprehensive patch management program. It's equally important to regularly backup your data. Before updating your software, create a backup to ensure that you have something to restore from in the event of a system failure or memory corruption during the update process. This step is vital for protecting your corporate data, whether it's your user's personal information or sensitive business data.

To create a sustainable patch management program, a culture of cybersecurity awareness must be fostered across the entire workforce. This involves educating IT staff about the importance of software updates and backups, as well as providing the end users with clear guidelines and best practices for maintaining system security. By engaging everyone in the process, we can ensure that users are not only aware of their role in protecting themselves and others but are also motivated to take the necessary actions to maintain a secure environment.

Fundamentally, a sustainable and effective patch management program hinges on a people-centric approach, communicating the importance of individual actions in maintaining a secure digital landscape. By focusing on software updates, system reboots and regular data backups, you can create a sustainable patch management program that is both effective and easily maintained END

Harman Singh

Managing Consultant and Director, Cyphere

Harman is a security professional with more than 10 years of consulting experience across private and public sector organizations. His day job involves serving his consulting business customers at Cyphere to reduce their security concerns.

@DigitalAmli

Patches are bug fixes, security fixes or even new security features in products that help prevent threat actors harming your devices. This is why patches are essential and often cited as the top recommendation to secure technology.

Patching every vulnerability is not possible. The answer lies in understanding the tricks of the trade – new, battle-tested techniques that can help ensure your systems are patched to maintain a minimal attack surface.

We Must Get off the Patch Everything Treadmill

Patch everything is never-ending cycle that's a de-facto recommendation often found in scanner reports or even penetration test reports. However, this is not practically achievable when it comes to fixes. The real homework for an organization starts after a penetration test when the risk remediation cycle begins. In reality, this is impossible to finish because of the amount of vulnerabilities coming out every month.

The first step is asset management, knowing what systems you manage, their underlying data and the business requirements these systems support.

With an up-to-date understanding of which services are exposed and what could be vulnerable, you'll have greater insight.

Knowing when certain systems become obsolete or unsupported helps you plan for upgrades before trouble strikes.

Automatic updates are an effective technique on mobile devices or cloud-based services where automatic patching and updates are turned on. There are no real challenges here except if settings are manually changed or disabled, and that can be taken care of by modern mobile device management solutions.

With limited financial resources and an overwhelming number of vulnerabilities, it can be difficult for organizations to prioritize patching. That's why risk assessments are critical – these guide the security team towards choosing which updates will have the most significant positive impact on their overall cybersecurity posture.

Risk-Based Patch Management Plan

The three most important factors to prioritize to ensure the effectiveness of a patch management plan are:

Criticality of the affected systems: Not all systems are equal for the organization. The importance of the system to the security and operations of your business defines the criticality factor. More critical systems should be prioritized for patching, as they can play the biggest role in decreasing attack surface.

Exploit likelihood of the identified vulnerability: Vulnerabilities can be exploited in different ways - some are easier to exploit, while others have more complexity due to environment metrics and associated dependencies. Identifying this likelihood helps determine how likely a host will be attacked or compromised.

Impact of the attack: A compromised system or service can have a massive impact on your organization. Identifying the risks associated with compromised system, like financial losses or data theft, will help decide which patching should be prioritized.

When Patching is Impossible

Scenarios where patching is hard or not possible may include systems in use but someone else is responsible for or legacy systems or services.

An organization can utilize related cybersecurity foundations to trust; these include but are not limited to:

- Managing operational risks, ensuring reduced ways to exploits because of secure architecture and configuration baselines
- Business critical data securely backed up and tested
- Incident response and business continuity capabilities END

API SECURITY

WHY DIGITAL TRANSFORMATION IS DRIVING A NEW WAVE OF RISK

Phil Muncaster explores how the fight to stay competitive is exposing a growing number of firms to cyber risk

If digital transformation is the direction of travel for most global organizations post-pandemic, application programming interfaces (APIs) have become a critical building block. APIs provide the glue that sticks together disparate software components, to create more seamless, connected experiences. But by coupling applications with backend databases to exchange information, they can also provide a pathway for cyber-criminals to access and steal sensitive corporate data.

This matters, as APIs become an increasingly ubiquitous part of software development – from healthcare to financial services. Nearly two-thirds (65%) of developers say they relied more on APIs in 2022 than the previous year – a trend only likely to continue. However, if organizations do not improve their visibility and control of the API environment, there could be trouble ahead. One 2022 report from Imperva and global insurer Marsh McLellan estimates average annual global losses to avoidable API security mistakes at $41-75bn. It's time to regain control of API security.

Why Organizations are Taking the API Approach

In a business climate increasingly characterized by uncertainty, intense competition, and macro-economic and geopolitical volatility, organizations are attracted by the idea of the "composable enterprise." First coined by Gartner, the approach posits that organizations break down their applications into components known as packaged business capabilities (PBCs). In so doing, they'll be better able to adapt to changing market conditions with speed and agility, to stitch these components together in various configurations. APIs are a critical part of a PBC, allowing developers to piece together these components as they wish. The growing popularity of modular, reusable microservices architectures can be seen in this context.

APIs and composability don't just help organizations to build from internal resources. They also support third-party integrations with partners, to create the connected experiences customers are crying out for. Organizations unwilling or unable to integrate into new value chains like this will increasingly see digital innovators move in on their turf. Open banking is a good example of where this kind of innovation has been forced on a conservative industry by new regulation. Mandated by the second European Payments Directive (PSD2), it has forced financial institutions to make available customer data to third parties via open APIs.

The result? API use in financial services grew by 125% between 2020 and 2021, according to Imperva. In other sectors, the surge has been even greater. API use in healthcare soared by 400% over the same period, while health monitoring increased 941% between 2021 and 2022.

Security Risks Associated with APIs

Unfortunately, these efforts are also expanding the corporate attack surface and providing threat actors with new opportunities. It doesn't help that many organizations aren't accurately tracking their use of APIs or updating security

policies and processes accordingly, according to Forrester principal analyst, Sandy Carielli.

"A lot of traditional web app security tools didn't support APIs, leaving holes in protection. Even as API security has evolved and more solutions are available, organizations struggle to understand what combination of tools and processes are needed," she tells *Infosecurity*.

"While the tools and processes exist to counter this threat, many organizations struggle due to the newness of the technology and the number of APIs in their organization. It's not uncommon for enterprises to have tens of thousands or even hundreds of thousands of customer and partner facing APIs – and they may not have a good grasp of what those APIs are and what they do," she adds.

That partly explains why the percentage of API traffic classed as malicious almost doubled between December 2020 and June 2021, from 1.4% to 2.6%, according to the analyst firm. A separate Salt Labs study last year found 94% of companies suffered security incidents in production APIs over the previous 12 months.

There are dozens of ways hackers can exploit an API, with OWASP the best resource detailing them all. Its latest top 10 list for 2023 features broken object level authorization (BOLA) as the most common attack type.

"[BOLA] occurs when an API client can access data it shouldn't be able to," Imperva director of technology, Peter Klimek, tells *Infosecurity*.

"Put simply, BOLA happens if someone requests an object and the API fails to verify whether they should have access to it. BOLA can lead to data theft, modification or deletion, depending on the APIs and vulnerabilities involved. Crucially, it only requires an attacker to be aware of the problem – no code hacks or stolen passwords are needed."

> ***"A lot of traditional web app security tools didn't support APIs, leaving holes in protection"***

Second on the OWASP list is "broken authentication" – where attackers take advantage of the "complex and confusing mechanism" for API authentication. OWASP warns that APIs must be treated differently from regular endpoints and given extra layers of protection. Often, that protection is implemented in a way that is misaligned to the relevant attack vectors and use cases, the non-profit argues. Rounding out the top three threats for 2023 is broken object property level authorization (BOPLA), which covers attackers gaining unauthorized access to sensitive info by manipulating endpoints – via "excessive data exposure" or "mass assignment."

"Excessive data exposure is when an API responds to a request with more data than necessary, allowing attackers to steal data. It can often occur if multiple applications share an API and the API relies on the clients to filter the data they need," explains Klimek.

"Each vulnerability is problematic in isolation, but when combined they can have devastating consequences for a business. Many of the largest API data breaches in history have been the result of an API being vulnerable to both BOLA and excessive data exposure."

Imperva's joint report lists the information sector, professional services, retail and finance as the four most frequently targeted verticals, with 57% of all API-related events reported in the US. It appears primarily to be a challenge for large enterprises at present. Most events occurred in companies with less than $50m in annual revenue, although those earning more than $100bn attributed roughly 25% of their cyber-events that year to API security issues.

How Firms Can Take Action

With APIs representing an ever more important part of the enterprise digital fabric, managing risk at this layer is an increasingly critical part of the corporate security strategy. Forrester claims in its report that 43% of those planning to adopt API security are looking to deploy in development, where it's cheapest to remediate and easiest to identify the API owner. However, a fragmented security market may complicate these efforts.

"CISOs should combine process and technology. Good API governance helps manage the plethora of APIs, and API discovery tools will help you find rogue or shadow APIs," says Forrester's Carielli. "Implement API protections in web application firewalls (WAFs), bot management and socialized API security tools to analyze API requests and block malicious ones. API gateways help with authentication and authorization."

For Imperva's Klimek, visibility is the essential foundation of good API security.

"First, make sure SecOps and DevOps communicate and collaborate with one another. Key to this will be an effective feedback loop between the two teams, allowing them to work in concert and streamline workflows while also ensuring security visibility and control," he says.

"Second, organizations need to embrace automation to ensure security standards and practices are met at all stages of the development lifecycle. Third, machine learning is a key requirement – especially when dealing with API abuses like BOLA, which cannot be detected or mitigated through signature-based detection mechanisms."

Andy Tyler, senior penetration tester at consultancy Bridewell, argues that although major improvements have been made in API security, automated in-house scans are often riddled with false negatives.

He tells *Infosecurity* that secure design is critical, to ensure that security teams aren't overloaded with time-consuming work fixing poorly planned APIs after the event.

"You need to make sure your team can identify the pitfalls and where to find best practice guidance in order to avoid common mistakes. The OWASP API Security Project is a great starting point, and there are many other great resources for this publicly available," he concludes.

"Monitoring traffic and identifying malicious intrusion attempts is also very important. However, it can be a daunting task given that APIs are expected to see high-volume traffic when used normally. Through effective logging, setting sensible alerts on anomalous traffic and making sure those who see the alerts know how to identify real threats, you gain great insight into the security of your API and the ability to respond when needed." END

Top Five API Security Issues

OWASP's API Top 10 list for 2023 was still being finalized at the time of writing. However, the upper half of the list featured the following:

1) Broken Object Level Authorization (BOLA): API fails to verify whether a requester should have access to an object.

2) Broken Authentication: Missing and/or mis-implemented authentication protections.

3) Broken Object Property Level Authorization (BOPLA): Attackers are able to read or change the values of object properties they are not supposed to access.

4) Unrestricted Resource Consumption: Multiple concurrent API requests can lead to denial of service.

5) Broken Function Level Authorization: Attackers send legitimate API calls to an API endpoint that they should not have access to.

TOP TEN Open-Source Vulnerabilities

01
CVE-2022-0543. Severity: CRITICAL

Located in Redis on Debian-specific (Debian, Ubuntu) distributions of Linux that use the Lua engine, this vulnerability can enable attackers to escape the Lua sandbox to achieve RCE.

CVSS Base Score: 10

02
CVE-2022-29464. Severity: CRITICAL

This vulnerability is an unrestricted arbitrary file upload vulnerability in various WSO2 products. It can be exploited by an unauthenticated remote attacker by uploading a specially crafted Jakarta Server Pages file to a vulnerable server.

CVSS Base Score: 9.8

03
CVE-2022-0811. Severity: HIGH

Discovered in CRI-O v1.19 container runtime, this vulnerability allows for container escape and gaining root access on the host, letting the attacker move freely in the cluster. The threat actor must have rights to deploy a pod on a Kubernetes cluster to exploit it.

CVSS Base Score: 8.8

04
CVE-2022-0185. Severity: HIGH

A heap-based buffer overflow found in the Filesystem Context functionality of the Linux kernel, this flaw can lead to an unprivileged user escalating their privileges.

CVSS Base Score: 8.4

JAMES COKER

Top Ten: Open-Source Vulnerabilities

The growing use of open-source software across digital services and products carry with them major cyber-risks. In essence, open-source software is open to everyone for any purpose, making it easier for threat actors to discover and exploit vulnerabilities in its code.

It is crucial that the cybersecurity industry, governments and the open-source community collaborate closely to quickly identify, communicate and remediate vulnerabilities in this software.

***Infosecurity* has compiled a top ten list of the key open-source vulnerabilities discovered in 2022. The data comes from the Tenable 2022 Threat Landscape Report, with the vulnerabilities ranked according to the Vulnerability Priority Rating (VRP) calculated by the vendor (0-10). This is based on both the impact and exploitability of the vulnerability.**

Vulnerabilities without CVEs in the National Vulnerability Database (NVD) do not receive a VPR score.

05
CVE-2022-0847. Severity: HIGH

This improper initialization vulnerability is located in the new pipe buffer in the Linux kernel. Exploitation can lead to the improper preservation of permissions.

CVSS Base Score: 7.8

06
CVE-2022-0492. Severity: HIGH

Another flaw in the Linux kernel, this improper authentication vulnerability requires specific configuration to facilitate exploitation. When exploited, it can allow an attacker to escape a container and escalate privileges.

CVSS Base Score: 7.8

07
CVE-2022-24348. Severity: HIGH

A path traversal vulnerability in Argo CD, attackers can create a malicious Helm chart to consume YAML as value files. To exploit the flaw, a threat actor must have permissions to create or update applications that can either guess or has knowledge of the full path to a file containing valid YAML.

CVSS Base Score: 7.7

08
CVE-2021-3998. Severity: HIGH

This is a vulnerability in the realpath() function of glibc in the Linux kernel that can lead to information leakage or sensitive data disclosure.

CVSS Base Score: N/A

09
CVE-2021-3999. Severity: HIGH

Another flaw found in glibc, this is an 'off-by-one' buffer overflow and underflow vulnerability. If the buffer size is 1, a local attacker could leverage the vulnerability to execute arbitrary code or elevate their privileges.

CVSS Base Score: N/A

10
CVE-2022-3602. Severity: HIGH

This buffer flow vulnerability in OpenSSL can, when exploited in uncommon environments, enable attackers to achieve RCE. The flaw caused by a function that verifies x.509 certificates.

CVSS Base Score: N/A

SLACK SPACE

Grumbles / Groans / Gossip

01 Beware of Teenagers

Teenagers and young adults in their 20s are among the most prevalent threat actors targeting US organizations today, according to Mandiant's Charles Carmakal.

The CTO of Google Cloud's Mandiant Consulting said his threat intelligence team has been "tracking a number of [teenage] groups, […] who live in the US and the UK, who typically speak English as their first language and who are incredibly effective social engineers."

"They are able to convince people to do things they ask them to do, like visit certain malicious websites and type in their username and password, or log into any desktop comm and download the AnyDesk client and provision access to somebody," he added, while speaking at the RSA Conference in San Francisco on April 24, 2023.

He said that some of them broke "into some of the biggest organizations by leveraging these techniques that are so hard to defend against."

One of these groups, now allegedly defunct, was called Lapsus$ and was responsible for leaking information from the likes of Okta, Nvidia, Samsung, Ubisoft, T-Mobile, Microsoft, Uber and Rockstar Games, among others – in 2022 alone.

Some of the Lapsus$ gang, including its alleged ringleader, were arrested in March 2022.

Another campaign, linked to the Okta hack and run by a threat actor Group-IB called Oktapus, compromised more than 10,000 user credentials across 136 organizations in the summer, including Twilio and Mailchimp.

What is scary about these groups, Carmakal continued, is that they conduct their extortion in a way that is very different to how most ransomware groups do it.

"They are making it very personal. If you think about the dynamic in extorting an organization, it's one thing to pay a threat actor to get a decryptor to get your systems running again. It's a very different story if you're an executive at the company and your daughter is being harassed by a threat actor. Your desire to pay, or your willingness to pay shoots up ten-fold."

02 Flipper (Almost) Exits Amazon

Flipper Zero is not just a Tamagochi-looking gadget; it's also a hacker-favorite, versatile penetration-testing tool.

Unfortunately for the cybersecurity hobbyists that Flipper Zero's creator Alex Kulagin devised it for, the device is no longer available on the US website of Amazon's marketplace.

The reason for that seems to be the tool's capacity to emulate NFC data, which means that cards or devices in proximity and broadcasting on the 13.56 MHz band could be read and potentially emulated without the owner's knowledge.

Card skimming, as this practice is commonly called, is illegal in many jurisdictions.

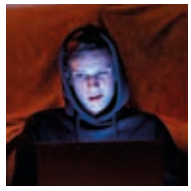
It is also registered as a prohibited practice in Amazon's blacklisted devices, along with lock picking and theft.

However, this scenario is improbable, as the odds of a user actually cloning all required meaningful data from an unsuspecting victim's credit card are currently impossible. Indeed, Flipper Zero cannot read the additional encrypted data on bank cards that would allow it to complete a transaction.

Flipper Devices' CEO Pavel Zhovner previously told BleepingComputer that the company asked Amazon to reconsider the ban as the device is incapable of skimming bank cards.

At the time of writing, Flipper Zero remains unavailable on Amazon in the US but can be found on France's, Germany's and the UK's versions of the marketplace.

In March 2023, Brazil's National Telecommunications Agency (Anatel) started seizing incoming Flipper Zero purchases based on its alleged use by criminals.



1. *Is the hoodie back in fashion?*

2. *Or you can buy it on Flipper's official website*

3. *Infernal Affairs*

03 US-Based Chinese Expats Scammed by Fake PRC Officials

Criminal actors posing as Chinese law enforcement officials are extorting money from US-based Chinese individuals, the FBI warned in an advisory published on April 10, 2023.

Using fake identities, such as agents of China's Ministry of Public Security or Chinese consulates in the US, the criminals typically call Chinese nationals living in the US, sometimes using spoofed numbers, accuse them of financial crimes and threaten to arrest or hurt them if they don't pay.

To substantiate their claim, the crooks use basic knowledge about China and Chinese culture and, in some cases, "show victims fraudulent documents as proof of these accusations, including realistic-looking arrest warrants or intricate details about alleged criminal schemes," reads the warning.

According to the FBI, this scam leverages "widely publicized efforts by the People's Republic of China (PRC) government to harass and facilitate repatriation of individuals living in the United States."

Here, the Bureau is likely referring to 'Operation Fox Hunt,' a program started in October 2022 by the Chinese Communist Party to hunt down Chinese citizens living abroad and return them to the country.

The PRC claims this operation is designed to catch corrupt wealthy Chinese individuals living abroad, including in the US, Canada and Europe.

According to the FBI, PRC officials can go as far as to pressure and threaten their targets' relatives to convince them to return to China, send threatening letters, sue them in US courts and send covert teams to stalk and harass them.

The Bureau recommended that anyone contacted by an alleged foreign authority reach out to their local FBI field office. "Foreign government officials conducting legitimate law enforcement activity in the United States must act in coordination with US federal authorities," reads the advisory.

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

Parting Shots...

James Coker, Deputy Editor

The launch of OpenAI's ChatGPT in November 2022 has sparked a huge amount of discussion and debate around the role of AI in society – often in a negative light.

Yet the field of AI is certainly nothing new to cybersecurity professionals, and automation has played a significant role in cyber-attack and defense tools for a number of years now.

Still, ChatGPT has led to a lot of discussion regarding the impact of generative AI in the industry. Worryingly, experts have warned about its potential to create malware and more sophisticated social engineering campaigns.

On the flip side, others have been encouraged by its ability to write secure code as well as debug existing code.

Unsurprisingly, these topics were heavily discussed throughout this year's RSA Conference, which took place in the beautiful city of San Francisco, California, from 24-27 April, 2023.

I had the pleasure of attending this event along with colleagues from *Infosecurity* Magazine, and it was fantastic to hear and speak to experts about this issue in a variety of contexts. A common message was that we need to cut through the hype around AI and understand its potential threats and opportunities in a calm, level-headed manner.

As with many aspects of the modern day, there seems to be a tendency to catastrophize and overstate in equal measure, and as a society we are starting to do that regarding AI.

In a talk at the RSA, a good friend of the magazine, Diana Kelley, highlighted how dystopian ideas about AI machines ruling over humans remain far-fetched. She also said it is important not to overplay AI's capabilities in cybersecurity, as this can lead to unrealistic expectations and potentially lead to apathy.

The reality, at this stage anyway, is far less dramatic. Speaking to me at RSA, BlackBerry's vice president of threat research & intelligence Ismael Valenzuela described generative AI as an "assistant" to the work of both attackers and defenders, rather than revolutionizing their approaches – that sums up the situation well in my view.

New Tactics

Another interesting talking point from the event is that cyber threat actors are being forced to find new ways to infiltrate organizations' systems due to improving solutions in areas like email defense.

While this clearly shows that defenses are working against old tactics, threat intelligence experts described how attackers have effectively leveraged alternative techniques in response to improving tools. One noteworthy approach that has become prominent in the past year is SEO-based attacks, whereby threat actors are using legitimate search engine services to push malicious websites to the top of search results. From there, they seek to infect the user's device with malware and infiltrate their organization.

This approach can overcome web blocking tools as it leverages well-known search engine websites. This technique is another example of the continuous cat and mouse game between attackers and defenders, and why cybersecurity teams can never rest on their laurels in their quest to keep their organization secure.

It will be fascinating to hear the discussion continue in these areas and more at our own Infosecurity Europe conference, which is being held at the ExCel, London, from June 20-22, 2023.

Alongside a range of industry-leading speakers already confirmed for the event's conference programme, the *Infosecurity* Magazine team will be busy producing our own content at the show, including in-person panels, interviews and breaking news stories. Please do keep an eye out for our activities while there – I can't wait for a fantastic three days of engaging with the cybersecurity community.

The cybersecurity industry is facing unprecedented challenges at the moment, with attacks surging in volume and sophistication – exacerbated by the unstable geopolitical landscape and resulting threats from nation-states. On top of this, security leaders are grappling with the impact of the global financial crisis, making it harder to get extra funding for their team from business owners.

Yet, as is often the case, innovation and creativity are most apparent in times of adversity, and this is something we are increasingly seeing – including around the use of AI and machine learning to reduce the burden on security professionals.

Startups are particularly known for thinking outside the box to find solutions for specific problems, and it is heart-warming to see this community thrive despite the turbulent economic headwinds.

Governments and large tech firms are recognizing the enormous value that startups provide to the cybersecurity industry, and we are seeing a number of accelerator programs emerge by these bodies to help new companies develop their products and scale.

With this in mind, the results of the UK government's 'The Most Innovative Cyber SME 2023' competition will be unveiled at Infosecurity Europe. Please do take time to check out these companies, who will be exhibiting at the event, to see how their innovative ideas can boost the industry.

Thank you for reading this edition of *Infosecurity* Magazine, and I look forward to seeing many of you at Infosecurity Europe in June!

Best wishes,

James Coker END

Infosecurity Magazine

SUBSCRIBE

To keep up to date with the latest news, insights and events, view upcoming and on-demand webinars or download white papers and reports make sure you subscribe to Infosecurity Magazine.

"Uncover the power of infosecurity"