Infosecurity Europe challenges CISO community to predict top trends and challenges for the industry in 2019

Security by design, critical infrastructure flaws, and closing the gap between the C-suite and IT security function all top the list

Richmond, Surrey, UK, 0900 hours, 12 December 2018 – As 2018 draws to a close, Infosecurity Europe 2019, Europe's number one information security event, has challenged its CISO community within financial services and other key industry sectors to predict the trends that will shape the industry in the year ahead.

With the information security market forecast to grow by 8.7 per cent to $124 billion in 2019, according to Gartner[1], many of the same challenges are keeping senior security professionals awake at night, with identity and access management, insider threats, third party and supply chain risks, and cloud still seen as top challenges for year ahead.

But, according to Victoria Windsor, Group Content Manager at Infosecurity Group, CISOs are not just focusing on technology issues, but also the human element: "There are concerns about the growing skills gap in the market and a paucity of skilled, talented individuals. The expectation is that the market will continue to grow as smaller companies emerge to fill the skills gap. The ever-changing role of the CISO is also top of mind and 2019 is predicted to be the year when cyber resilience takes its rightful place at the boardroom table. But more needs to be done to bridge the gap between the C-suite and IT function.

"2018 was the year of GDPR and the fallout from this is high on our CISOs' list, as regulators seek to enforce compliance. Vulnerabilities in critical infrastructure due to legacy control systems, and the role of security by design for product and application development (DevSecOps) to mitigate business risk also come under the spotlight."

Infosecurity Europe C-suite cybersecurity trends 2019:

One of the most targeted sectors when it comes to cybersecurity threats, the financial services industry saw an 80% increase in attacks in 2017, according to reports by the Financial Conduct Authority (FCA). But while the industry is one of the more resilient sectors, **George Luchita, Head of Cyber Security and IT Infrastructure, FM Capital Partners Ltd**, voices his concerns over the growing information security skills gaps and the impact post-GDPR:

"My personal view is that 2019 will be a dynamic year, just like 2018. We are going to see the effects of GDPR, as regulators will start enforcing it. Information security will penetrate deeper into boardrooms, with CISO roles created to effectively manage cybersecurity risks and gain market and reputational advantages. Cyber resilience will be present on boardroom agendas.

[1] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

The information security skills gap will increase, driven by increase in demand and lack of specialists. Companies will find it difficult to recruit and retain experienced and talented people. As a response to absence of sufficient infosec skills, we will see a rise in the number of small cybersecurity firms looking to fill the void. Regarding IoT, in 2019 we'll see an increase in the number of internet-connected devices, and we'll face more issues regarding their security. There are predictions of massive attacks using IoT devices, but I doubt it will happen next year. IoT has not yet reached a critical mass or wide adoption to enable such attacks."

Justin Campbell, **Director, Technology Consulting Services** at **Willis Towers Watson** highlights the importance of security by design and the role of DevSecOps in IT operations security to ensure faster and more secure software delivery:

"DevSecOps, security by design – built-in security. The time to market and the risk of finding major structural vulnerabilities at the late stages of product development or architectural deployment are too high. Rather than novel exploits for 2019, I see the biggest challenge is providing security value at the point of development or system design. Many security professionals come from an audit and compliance perspective. There will always be a place for these professionals in certification and reviews. However, when we find the faults at the end of the process, whether through checklists or pen tests, it is often too late. At this late stage, a product is often missing its deadline to go to market or a business case requires a quick go-live. This puts a business owner into an impossible predicament. He or she needs to accept the risk or lose their business position. This makes it too tempting to accept an inappropriate level of risk or rationalise away the situation with shaky mitigations."

While 2018 saw no repeat of 2017's WannaCry attack that affected hospitals across the UK, **Nigel Stanley, Chief Technology Officer - Global OT and Industrial Cyber Security CoE at TÜV Rheinland Group**, believes critical infrastructure will again be under the spotlight in 2019.

"I believe that in 2019 further significant cybersecurity flaws will be uncovered in key critical infrastructure resulting in manufacturers and operators trying to update ancient control systems with mixed results. I hope I am wrong, but I also believe that in 2019 we will see a safety critical incident that arises from a cyber attack on an industrial control system resulting in physical harm and damage. It is likely to be a sophisticated attack arising from a hybrid, geopolitical conflict. This will lead to further demands in 2019 for industrial cybersecurity and safety regulations to be tightened up and penalties for non-compliance increased. These future legal requirements will insist that industrial operators and systems' manufacturers address cybersecurity risk to the same degree they do with safety risks."

Finally, **Nick Carus, Business Development Director at LINQIT and Interim COO and Business Development Director at Caveris**, predicts that executives will finally start to talk and collaborate with the IT security function to help close the threat gap

"Good news GRC is leading from the front. I predict that the focus on 'Bridging the Gap' between the C-suite and the IT/technology organisations, and getting the executives more interactively communicating and collaborating with IT security and all infosecurity disciplines, simply has to happen over the short term. It's the only way that organisations are going to be able to make effective strides in closing the 'Threat Gap'."

Infosecurity Europe, now in its 24th year, takes place at Olympia, Hammersmith, London, from 4-6 June 2019. It attracts over 19,500 unique information security professionals attending from every segment of the industry, as well as 400+ exhibitors showcasing their products and services, industry analysts, worldwide press and policy experts, and over 200 industry speakers are lined up to take part in the free-to-attend conference, seminar and workshop programme - https://www.infosecurityeurope.com

Ends

About Infosecurity Europe

Strategically held annually in London, Europe's centre for technology start-up businesses, Infosecurity Europe is Europe's largest and most comprehensive Information Security event. Featuring numerous analysts, policy experts, journalists and over 400 exhibitors, Infosecurity Europe presents an invaluable business platform, as well as staging the world's largest complimentary conference programme containing 240+ free to attend conference sessions which have been accredited by leading industry associations (ISC)² and ISACA since 2012. The event attracts over 19,500 unique information security industry professionals attending from every segment of the industry and presents the most important date in the calendar for information security professionals across Europe. www.infosecurityeurope.com. @Infosecurity #infosec

For further information, please contact:
Paula Averley
Origin Comms
t. 020 3814 2941
m. 07766 257776
e. infosec2019@origincomms.com