CSO

IDG COMMUNICATIONS

IT complexity, hyper-connectivity and compliance: three challenges facing CISOs in 2020

Marga Verdú

Overlapping management of business demands, technological upheavals, a backdrop of constantly evolving threats and other barriers such as staff crunches and the need to comply with regulations, all makes for huge complexity to be faced by those in charge of IT security.

To coincide with Cisco Live 2020 – the EMEAR meeting that Cisco organizes every year – the technological giant has held Cisco **CISO Day** in Barcelona, a day in which almost one hundred chief information security officers (CISOs) from Europe, the Middle-East, Africa and Russia have gathered, and it has taken place at the Cisco Co-Innovation Center in the Mediterranean city.

In a speech focusing on the issues that most concern CISOs at present, and having held multiple talks with them in the past year, **John Maynard, Vice President of Global Cybersecurity at Cisco, underlined two issues**: *"Objective number one is protecting infrastructure, while ensuring that mechanisms shall be available to to provide resilience capacity in situations of network vulnerability."* Maynard pointed to the **Cisco Co-Innovation Center Center de Milan** as the specialty IT security hub where it is possible to participate and co-innovate

With the aim of backing up strategic security approaches in organizations, Cisco CISO Day has drawn on the support of experts in IT operations strategy to lead support sessions for security professionals' roles and achieving objectives.

with industry partners, clients and developers of solutions, by working together.

With regards to how he sees the future of security, John Maynard was convinced that it would depend to a great extent on the Internet of Things devices connected to networks, and **he called on security and privacy as two of the factors that cause most concern in organizations**, while stressing that; *"Digitizing cybersecurity will be the enabling element we need in order to work with with industry in securing those IoT devices that are connected to networks."* For Maynard, the advantages to be derived form privacy will provide financial returns. *"Privacy is an investment,"* he concluded.

When it comes to breaking down the key elements that form part of any IT security process that is assembled successfully, **Wendy Nather, Director of the CISO Experts Committee, Duo Security, at Cisco**, alluded to the importance of evolving as regards traditional firewall perimeters and parameters. *"When it comes to spotting infrastructure weaknesses, the level of cybersecurity that one organization must implement does not necessarily have to be the same as another in the same sector, in order to perform the same function. A study we conducted a couple of years ago made it plain that small-scale banks maintained an operations profile that had many elements in common with companies belonging to the retail business. Therefore* ***I would recommend that CISOs observe how security operations are adapted in business from other sec-***

Harvey Jang, Chief Privacy Officer at Cisco.

Simon Minton, Cisco Global Cybersecurity Advisory.

tors in aspects regarding the use of technology and how it impacts cybersecurity in their company's business." In Wendy Nather's view, organizations must have available experts that ensure the minimum required security level that they need, for which she recommends using third parties. *"Only 23% of companies trust staff when it comes to issues regarding advanced security,"* she explained in her speech. Meanwhile, Nather echoed that a good number of organizations struggle to maintain cybersecurity, even thought they earmark budgets of between 1 and 10 million euros a year on protecting their systems. *"The main barriers in place when adopting advanced security technologies are derived from budgetary constraints or pressing priorities that arise connected to the business,"* she pointed out.

Securing users, as well as jobs and workloads in multi-cloud environments poses challenges for many IT security directors that try to set up multi-domain security. As **René Raeber, Distinguished Engineer and CISO Alumni at Cisco**, put it; *"Given that both technology and threats have undergone various forms of extrapolation, convergence in cross-domain security represents that maximum aspiration in a universe of IT complexity such as we have now."* **This expert's view entails locating security much closer to the applications campus and data center, by undertaking segmentation and micro-segmentation operations with the aim of minimizing the possibility of surface attacks arising.** *"Active protection from attacks prevents breaches from being produced,"* he maintained. As a Distinguished Engineer and CISO alumnus at Cisco, he was in favor of using smart networks based on the intention that they be capable of supervising and reinforcing automated learning processes with the aim of safeguarding user activity, infrastructure and applications.

Engineers and developers working together on DevOps security

When broaching the topic of DevSecOps, which would correspond to the philosophy

John Maynard, Vice President, Global Security Sales at Cisco.

Chris Leach, Senior CISO Advisor at Cisco y Paul D'Cruz Ceng, Director of Cisco Security Operations EMEAR.

based on integrating security in the DevOps process, Simon Minton, Global Cybersecurity Adviser, opts for developers and software engineers working together. *"When engineers and software developers work with the same tools, we will manage to avoid the dreaded bottlenecks. That may be done by using the SRE (Site Reliability Engineering) platform for development teams,"* he said. Minton stressed that DevSecOps processes, by acting continuously, have the ability to provide a positive perception of security, and bring about environments that consolidate trust among work groups. *"Working with engineers will facilitate automation and compliance in cybersecurity processes,"* he maintained.

Zero Trust is a trend that has fully made itself felt in an industry well known by **Richard Archdeacon, a member of the Advisory CISO team at Cisco EMEAR.** *"Aspects that distinguish the Zero Trust approach (zero trust outside the network) regarding traditional security systems addresses the possibility of enabling secure access by cutting the risk of attack."* According to Archdeacon, Cisco has developed a practical methodology for defining and implementing the latter security model. *"Using Cisco Zero Trust, organizations have available a holistic protection model for all accesses and it puts on the table a system that gives an idea of the way in which security is applied, by providing the basic elements to transform the protection methodology that meets business challenges and demands."* By focusing on staff, jobs and workloads, Cisco Zero Trust forestalls threats and has the ability to discover new weaknesses and unknown malware.

From an outlook focusing on the role of security directors, **Michael Jenkins, MBE y CISO at Brunel University, London,** and author of crime and spy novels, underwent a journey through intelligence and cyberterrorism operations, using narratives that deal with hybrid threats doing the rounds of networks nowadays, and that provide clues for officers when taking decisions for organizations concerning the type of investments

Lothar Renner, Managing Director, Cybersecurity Sales and Engineering, EMEAR at Cisco.

to be made at the board of directors' level. ***"The culture regarding data handling has not been strict enough, which is a worry when bearing in mind that this practice has led to numerous incidents, particularly phishing and intruding on networks.*** *Universities have very valuable information assets available that could make a big impact at the national level if they were to fall into the wrong hands, due to the amount of information regarding research programs, intellectual property, patents and personal data,"* he warned.

To understand how operational efficiency reduces complexity in this dynamic panorama of cyberthreats, **Paul D'Cruz Ceng, Director of Security Operations EMEAR at Cisco,** and **Chris Leach, Senior CISO Adviser at Cisco EMEAR,** referred to the benefits to be derived from using an open and integrated platform to reinforce operations and generate efficiencies in business processes. These two experts were unanimous in pointing out the advantages of using an integrated architecture in corporate management that incorporates SIEM (security information and event management) and SOAR (security orchestration, automation and response) tools. *"These elements will undertake key actions in advanced security, for they will allow for determining whether the complexity of the operations environment prevents process solution; whether fatigue is added to tools, processes and applications due to handling a great number of devices or processes, to an increase*

IT challenges and priorities from the perspective of CISOs

IT security officers have much to say about the priorities, complexities, challenges and opportunities arising from the current situation in business security. For most CISOs attending the Cisco day, some of the challenges they had to face in 2019 had to do with hunting and retaining talent from the human factor standpoint, the demand to integrate OT cybersecurity platforms that come with integrated security tools, levels of security that do not interfere with user experience and staying within budget.

As far as priorities for 2020 are concerned, some have warned of the risk entailed in increasing connectivity, although they call for setting up geopolitical regulations and mechanisms capable of encrypting, monitoring and banning devices. From a consumer privacy point of view, CISOs welcome regulations such as GDPR while they recommend strengthening consent over data use and the possibility that misuse of user information may affect the reputation of a particular brand. Meanwhile, CISOs recommend developing an IT culture geared to preventing risks regarding users, while most acknowledge the barriers that separate CTOs from CISOs in many companies due to issues arising from cybersecurity.

in time or budget; or specialization that focuses too much on one or two solutions for the majority of technicians faced with the latter's lack of familiarity with other techniques," Paul D'Cruz noted.

For his part, **Lothar Renner, Managing Director Cybersecurity EMEAR at Cisco,** echoed the looming priorities and challenges for IT security professionals. *"CISOs need to strike a balance between security, privacy and meeting compliance terms, while they must commit to continual innovation."* Therefore, Renner asserts that visibility will enable security directors to be aware of the elements exposed in order to protect them. *"To ensure infrastructures that operate in multiple environments, Cisco's response entails integrating DevSecOps,"* he stated. According to this expert, it is also worthwhile appealing to common sense when dealing with protecting infrastructure, by always verifying origin and never trusting in appearances. *"On the strategic plane,* ***CISOs will be well advised to move on from a strategy based on 'adopting the best security on the market' to another based on integrating protection elements wherever necessary,"*** he recommended.

To round off the CISO Day 2020 in Barcelona, the **Head of the Barcelona Co-Innovation Center at Cisco where Cisco CISO Day was made, Xavier Azemar,** was entrusted with valuing the existence of old premises such as Ca L'Alier, a textile mill that opened in the mid-nineteenth century that, after eight years' rebuilding work, has become an IT innovation center. *"This center that Cisco has set up in Southern Europe will be the IT co-innovation hub in which the basics will be established for everything related to smart cities. In addition to coining the term and laying the foundations for Fog Computing, Cisco has committed, along with the city of Barcelona, to developing an efficiency and sustainability policy for the co-innovation building itself that it runs in that city, while setting up a link between activities at the Cisco Co-Innovation Center and the legacy of quality and innovation that have always been hallmarks of activities undertaken by Barcelona city hall in the district comprising area 22"*. Azemar likewise pointed out that the Cisco Co-Innovation Center is based on five strategic pillars: development, acquisition, investing with partners and co-innovation in solutions geared to the IT ecosystem. **CSO**

ADDITIONAL CONTENT

Access the summary and more content of the event here

Learn more at cisco.com/uk/secure