Hong Kong
December, 2017

Synthesis

Egon Zehnder Cybersecurity Roundtable, Hong Kong

EgonZehnder

Egon Zehnder recently held a Cybersecurity Roundtable Discussion in Hong Kong, moderated by Richard Lin and Matthew Edwards, consultants in our Technology Officers and Fintech practices. We were joined by Sean Duca, Chief Security Officer of Palo Alto Networks Asia, and by twelve CEOs, CIOs, and CISOs from leading financial services, telecommunications, consumer, transportation, and government organizations. We enjoyed an in-depth discussion and open exchange of ideas, insights, and best practices related to all things cybersecurity. We've shared some of the most significant takeaways below:

Cybersecurity awareness and education

Cyberattacks are growing in frequency, sophistication, and impact. Adding to the challenge are employees who are not cautious about cyberattack attempts and expose themselves to phishing, password theft, and other intrusions. Consequently, educating staff to increase awareness and vigilance is now crucial. In our discussion, panelists described some of the best practices they are employing at their companies, such as having regular training on data safety and running tests on employees through mock attacks. In some cases, the practice is taken so seriously that employees who repeatedly fail to respond appropriately to mock attacks are reprimanded and sometimes even terminated.

Intelligence sharing and its challenges

While panelists generally agreed that information-sharing on cyberattacks and their possible prevention is an important way to enhance defense measures across industries, it is clear that challenges remain. One clear observation was that the various perpetrators of cyberattacks are often more coordinated than the industries that are the targets of their attacks. This is because of competition between industry players and a fear of leaking news of attacks to the media.

Our participants pointed out that depending on how cooperative the board is, CEOs and CIOs may believe the short-term reputational risk in sharing information on attacks outweighs the potential long-term benefits of being more transparent. Trust can be especially hard to build among industry peers, particularly among financial intuitions where client confidentiality is paramount. There was nonetheless general agreement that practitioners

can and should do better in sharing information, and it was suggested that support through government regulation could help.

Raising management awareness of cybersecurity risks

Data protection ultimately helps businesses reduce risk. Compared to just a few years ago, there has clearly been a shift in the awareness of cybersecurity among C-level executives and boards. However, there are varying levels of understanding among organizations. Some attendees were sleeping well at night, knowing that effective investments and policies for cybersecurity were in place. Other attendees noted that CIOs still need to invest a significant portion of their time in raising awareness within their organizations so that the whole management team fully appreciates the importance of IT security, with appropriate budgeting and headcount.

Third-party service providers and contractors

Some companies may realize they cannot grow their in-house IT capabilities at the same pace at which the overall business grows. They are therefore using third-parties to supplement capabilities and control costs. This may result in data risks that are beyond the company's control. While contracts and policies can be put in place to mitigate those risks, in reality there are challenges associated with maintaining appropriate cybersecurity standards through contractors. It is critical to establish trust—along with a sound legal framework.

Data protection measures

The pattern of attacks can be random in nature and initiated by individuals, groups, or nation-states. Apart from building up strong defenses, some companies have also taken proactive initiatives such as creating "honey pots" to lure hackers into their networks, all in an effort to better understand and learn from their strategies and therefore avoid future such attempts. Attendees shared examples of how cyberattacks could even result from an unflattering piece of public news that may encourage a disgruntled or activist cybercriminal to launch an attack.

CISO reporting line

This depends on the industry nature and business size. In some situations, the CIO is also the de facto CISO and reports directly to the CEO. This is especially

common in the technology and financial industries where the need for high-level cybersecurity is more pronounced. In some other organizations, CIOs or CISOs may report to a COO or CFO, with a dotted line to the CEO. Still, other organizations emphasize the legal implications of cybersecurity with the CISO reporting into the General Council of Chief Legal Officer. Smaller businesses may combine the CIO, CISO, and CTO roles into one. What appears most important is for the CISO function to have a strong voice at the top of the organization as cybersecurity becomes a bigger issue requiring strategic rather than financial oversight.

Legal and regulatory framework

Hong Kong law does not require companies to share much information regarding cybersecurity, and relevant cybersecurity and IT infrastructure legislation is not well established. This is something that can be improved upon. Panelists agreed that a good example is Singapore, where the government and legislators have established a strong regulatory framework for cybersecurity.

EGON ZEHNDER'S TAKE

While in most organizations, de-facto cybersecurity leadership continues to be vested in the CIO organization, the CISO function has expanded well beyond the realm of just "Racks and Stacks." To face increasingly complex cybersecurity challenges, a CIO or CISO must not only understand and address technology issues, but crucially must be a business leader who is highly effective at influencing the broader culture of the organization. As a result, our assessment of cybersecurity leadership talent increasingly focuses on those who can take a holistic approach to cybersecurity, treating it as a broader business issue that involves culture, practices, and people *in addition* to the technology. We therefore believe it is critical to look at the underlying drivers of curiosity, learning orientation, insightfulness, and engagement in selecting cybersecurity leaders for the challenge ahead.

For other Egon Zehnder articles on this topic, please see
www.egonzehnder.com/industries/technology-communications/cybersecurity

Moderators

Richard Lin
Hong Kong and Shanghai
richard.lin@egonzehnder.com
+852 2918 7611

Richard Lin, *based in Hong Kong and Shanghai offices, leads Egon Zehnder's Technology and Communications Practice for Greater China and advises technology, telecommunications, and new-media clients in executive search, assessment and leadership development. He is active in the Semiconductor; Systems, Services, and Software; and Digital segments and is a member of our Technology Officers Practice.*

Matthew Edwards
Hong Kong
matthew.edwards@egonzehnder.com
+852 2918 7688

Matthew Edwards *leads Egon Zehnder's Private Equity, Asset Management, FinTech, and Financial Officers practices in Hong Kong. He has deep experience in investment, wealth, and asset management across multiple countries, and is also active in the firm's talent assessment and leadership advisory services.*

Since 1964, Egon Zehnder has been at the forefront of defining great leadership in the face of changing economic conditions, emerging opportunities and evolving business goals. With more than 450 consultants in 68 offices and 40 countries around the globe, we work closely with public and private corporations, family-owned enterprises and non-profit and government agencies to provide board advisory services, CEO and leadership succession planning, executive search and assessment, and leadership development. For more information visit www.egonzehnder.com and follow us on LinkedIn, Twitter, and Instagram.

Amsterdam
Athens
Atlanta
Bangalore
Barcelona
Beijing
Berlin
Bogotá
Boston
Bratislava
Brussels
Budapest
Buenos Aires
Calgary
Chicago
Copenhagen
Dallas
Dubai
Düsseldorf
Frankfurt
Geneva
Hamburg
Helsinki
Hong Kong
Houston
Istanbul
Jakarta
Johannesburg
Kuala Lumpur
Lisbon
London
Los Angeles
Luxembourg
Lyon
Madrid
Malmö
Melbourne
Mexico
Miami
Milan
Montreal
Moscow
Mumbai
Munich
New Delhi
New York
Oslo
Palo Alto
Paris
Prague
Rio de Janeiro
Rome
San Francisco
Santiago
São Paulo
Seoul
Shanghai
Singapore
Stockholm
Stuttgart
Sydney
Tel Aviv
Tokyo
Toronto
Vienna
Warsaw
Washington, D.C.
Zurich