Cybersecurity: What Boards Need to Know

One of the sessions of Egon Zehnder's Directors Development Program addressed the multifaceted challenges of cybersecurity in a world that is becoming more technology driven and more connected. With a focus on cybersecurity risks and how the board can address them, the session was hosted by **Rahul Tyagi**, co-founder Safe Security, one the world's largest cybersecurity assessment company, and **Nandkumar Saravade**, former CEO of ReBIT and a renowned authority on data security.

Navigating the Complexities of Cyber Threats: Building a Human Shield

Tyagi initiated the discussion by providing a comprehensive overview of the current cybersecurity landscape. He underscored that cybersecurity is a real and urgent threat. "Cybersecurity challenges are not futuristic; they are unfolding in the present," he stressed, setting the tone for a discussion that would delve into the nuanced tactics employed by cybercriminals.

One of the key aspects of this issue, as Tyagi highlighted, was the profound impact that cybercrimes can have on individuals and organizations. "The impact of the crime, when executed in a nice way, can have a very, very big ripple effect in both your personal and professional life," he warned, highlighting the ripple effect that extends far beyond the initial breach.

Tyagi provided practical insights into the evolving strategies employed by cybercriminals, shedding light on the role of personal assistants in facilitating cybercrimes. In a world where online workplace collaboration is the norm, criminals leverage colleagues, personal assistants, and others who may not even realize the threat to gain unauthorized access to sensitive information. This underscores the need for heightened awareness and proactive measures to secure personal and professional digital spaces.

In a video demonstration, Tyagi showcased a real-life scenario where a cybercriminal, seated in a local

coffee shop, manipulated a company's domain to conduct a sophisticated email scam. The video illustrated the level of sophistication in modern cyber threats, emphasizing the imperative for individuals and corporations to remain vigilant. "Crime today is not happening from the basements; it can be happening from *anywhere*," Tyagi emphasized, dispelling the notion that cyber threats emanate solely from obscure locations.

Highlighting the evolving tactics of cybercriminals, Tyagi explained that many criminals no longer write malware themselves but specialize in tricking individuals into clicking on malicious links. He introduced the concept of "Evil-GPT," a term from the dark web denoting a jailbroken ChatGPT used to create malware. Criminals can now request customized malware code tailored to exploit specific technologies, exemplifying the automation and sophistication present in contemporary cyber threats.

Tyagi concluded with a cautionary note on the importance of details in cybercrimes. Referring to a scenario where a criminal altered a company's domain slightly to deceive key personnel, he emphasized that details matter to cybercriminals when crafting their malicious activities to compel people to click or take action. "It has to look familiar. This is where research is important. It's not some generic piece of spam. It's an email from their boss."

Another illustrative incident Tyagi shared involved a WhatsApp video call scam targeting a company executive. Despite the victim's innocence, the potential damage to the reputation and the challenges of containment showcased the far-reaching consequences of cybercrimes. Tyagi encouraged individuals to promptly report incidents for effective action, not being ashamed for falling into these scams.

Tyagi also extended his recommendations to organizational practices. He cautioned against the widespread use of non-secure messaging applications such as WhatsApp for corporate communications, stressing the legal implications and risks associated with such practices. On data protection compliance, for example, Tyagi highlighted the potential legal repercussions for individuals unintentionally containing company data in personal email accounts. He emphasized the importance of disabling certain features on messaging applications to prevent unintentional data exposure, particularly in the context of cloud backups.

> When it comes to cybersecurity, personal actions can affect organizations. Tyagi's insights painted a vivid picture of the evolving strategies employed by cybercriminals and the imperative for individuals and organizations to adopt proactive cybersecurity measures. By raising personal awareness, boards and organizations can build an effective human shield against cyber-attacks.

Strategic Approaches to Cyber Resilience at the Board

Transitioning from Tyagi's exploration of cyber threats, Saravade offered a broader perspective on cybersecurity challenges and strategic frameworks for resilience. He contextualized the discussion within the transformative role of technology, emphasizing that the advantages offered by IT are often eclipsed by the risks associated with cyber threats.

Saravade drew attention to the distinctive nature of cyber risks, noting that they stand apart due to the adversarial element. Unlike traditional risks like credit risk or market risk, cyber risks involve adversaries actively seeking to exploit vulnerabilities. "Cyber risks stand apart due to the adversarial element," he emphasized, setting the stage for a discussion on the collaborative and holistic strategies required to counter these risks effectively.

He also shed light on the highly automated nature of cybercrime activities. From phishing kits to the sale of high-value credentials, the level of sophistication in these activities demands a collaborative response that extends beyond the capabilities of individual organizations. "The fact is that everything is automated, and everything is easier to launch and becomes a big problem for people who are building the technology and trying to protect those," Saravade explained.

> For boards to address the challenge of cybersecurity, Saravade suggested adopting the NIST framework, a comprehensive standard that is widely adopted in the industry. "The standard framework for dealing with cybersecurity has been around for a long time now. It is called the NIST framework," Saravade stated, aligning the industry's strategic approach with regulatory guidelines.

Continuous risk assessment and quantification were also emphasized. Saravade advocated for a shift from qualitative to more scientific, quantitative approaches, stressing the need to understand the potential impact of cyber threats, aligning his insights with recent regulatory developments that demand prompt reporting of incidents. "In India, RBI has already been very rigorous about this. So 6-hour reporting timeline is there. And it is the initial intimation, then updates as they happen," he noted, underlining the urgency and transparency required in responding to cyber incidents.

In addressing cognitive biases and risks inherent in decision-making, Saravade touched upon the challenges faced by non-executive directors in accessing relevant information. He stressed the need for a focus on organizational excellence and discernment in navigating the information overload prevalent in the cybersecurity landscape.

For more information, contact:

Rahul Rana
New Delhi
rahul.r.rana@egonzehnder.com

Darpan Kalra
New Delhi
darpan.kalra@egonzehnder.com

Namrita Jhangiani
Mumbai
namrita.jhangiani@egonzehnder.com

Vineet Hemrajani
Mumbai
vineet.hemrajani@egonzehnder.com

About Egon Zehnder

Egon Zehnder is the world's preeminent leadership advisory firm, inspiring leaders to navigate complex questions with human answers. We help organizations get to the heart of their leadership challenges and offer honest feedback and insights to help leaders realize their true being and purpose.

We are built on a foundation that supports partnership in the truest sense of the word and aligns our interests with the interests of our clients. Our 560 consultants across 63 offices and 36 countries are former industry and functional leaders who collaborate seamlessly across geographies, industries and functions to deliver the full power of the Firm to every client, every time.

We partner closely with public and private corporations, family-owned enterprises, and non-profit and government agencies to provide a comprehensive range of integrated services, including executive search, leadership solutions, CEO search and succession, board advisory and diversity, equity & inclusion. Our leadership solutions cover individual, team and organizational effectiveness, development and cultural transformation. We work with world-class partners including Mobius Executive Leadership, a transformational leadership development firm.

We believe that together we can transform people, organizations and the world through leadership.

For more information, visit www.egonzehnder.com and follow us on LinkedIn and Twitter.