EgonZehnder

Synthesis

Cybersecurity and the Role of the Board

Banks urged to assess cybercrime risks

As part of the Directors Development Program, Egon Zehnder invited Saket Modi, Co-Founder and CEO of Safe Security, to speak on the emerging risks in cybersecurity and what board members should be thinking about. Modi, recognized in Fortune Magazine's 40 Under 40 list, Entrepreneur Magazine's 35 Under 35, and Forbes Magazine's 30 Under 30, was joined by his Co-founder Rahul Tyagi at the event.

As the annual global cost of cybercrime threatens to spiral to $10 trillion by 2025, banks urgently need to learn to assess and manage cyber risks effectively, declared Saket. The two co-founders presented a live hacking demonstration to show just how vulnerable both individuals and organizations can be to this ever-growing threat. Nowadays, you can even pay for an underground "hacker as a service," where you simply give the email ID of the person whose password or data you want. Two or three days later, you will be sent a screenshot showing that the hacker has logged into the inbox and you make a bitcoin transfer payment of $200 to $300.

Taking one recent example where an ATM switch as well as debit cards were hacked at a highly digitized cooperative bank so that money could be withdrawn without it being displayed on the bank balance, they demonstrated how these attacks are

staged and how difficult they may be to detect. In other cases, millions of dollars of cash are being siphoned out of mature banks, despite them spending billion-dollar budgets on cybersecurity.

> "The real concern, however, is about the damage to reputation and the loss of trust"

What may sound like something out of a movie plot is in fact a bitter reality. In other words, banks may be speeding ahead when it comes to digitization, but cybersecurity remains low.

Writing off the negative financial impact of $10 million or $20 million lost to hackers might be harsh. The real concern, however, is about the damage to reputation and the loss of trust, with regulators and notably with customers. This has a much more long-term effect, pointed out Modi. "After all, banks are all about trust as they ask customers to trust them with their money."

Eyeing up security

Most banks and financial services companies have started talking about security but they have yet to look at it in a structured way – and that is what is currently missing, he continued.

So, how do you look at risk management within banks? How can you technically assess cybersecurity risk? It all starts with defining roles and responsibilities. Here, the role of the Chief Financial Officer (CFO) is to illustrate the current financial position. Meanwhile the job of the Chief Information Security Officer (CISO) is to show the risk, not to own the risk. The Chief Risk Officer (CRO)'s job is to act as the cyber intent owner, with first line accountability for cyber risk management. The board, meanwhile, is responsible to hold management accountable. Meanwhile, business and IT falls completely under the CEO's responsibility. At the end of the day, ownership of the risk always lies with the business.

Furthermore, it's worth looking at cyber risk using some parallels from different industries. For instance, when you talk about credit risk, there are some well-established data science models which the banking and insurance industry use to calculate the credit risk they are taking on.

Cybersecurity is the No. 1 concern

> "According to the World Economic Forum, hacking is the number one concern for MDs and CEOs worldwide"

Many would expect rising inflation or a turbulent economy to be leaders' number one concern right now. The CEO of one $4 billion Indian company sees it differently – cyber security is his first and foremost concern. Recently, his company fell victim to a phishing attack, with a hacker stealing something known as the "golden ticket," basically the master key to the active directory, thereby gaining access to every single file from employee payrolls to their accounts.

This CEO is not alone. According to the World Economic Forum, hacking is the number one concern for MDs and CEOs worldwide, says Modi.

This is no surprise considering how sophisticated some phishing attacks have become. Even for security professionals it can be next to impossible to detect the legitimacy of an email and the domain through which it is sent. "The point we're making is that hacks are very real and it's pretty simple these days to go ahead and execute them and that's the reason why it's become the number one worry."

Being held to ransomware

In future, artificial intelligence will be employed to make hacking even more malicious. This can present itself as ransomware – a type of malware that prevents or limits users from accessing their system until a ransom is paid.

The next evolution is Doxware, a type of ransomware that threatens to release personal data, such as photos and a list of contacts to the public if the user doesn't pay the ransom.

Other advances include MITRE Kill Chain, which has been developed by the U.S. government as the kill chain of every hack that can possibly happen, starting from reconnaissance to persistence, defence evasion, lateral movement, data collection, and data exfiltration.

The way you calculate the likelihood of a breach is to see if the kill chain is doable or not, which techniques are failing and the ways to dynamically map it. There are

enough tools available to work out the costs. Notably in a ransomware attack, less than 10 percent of the amount spent is the actual ransom: the rest is made up of forensic costs, breach notification costs, legal expenses, PR expenses and the loss of reputation.

Knowing the risks

The top 25 CISOs in the world now use a simple yet comprehensive model known as the Interactive Cost Model to examine cyber risk. This firstly looks at your overall expected dollar loss based on all the controls currently in your environment and all the hacks that can possibly take place.

When you know the dollar risk, there are three ways forward. Either mitigate the risk, transfer the risk, or accept the risk. The board then decides if the residual risk is acceptable or too high and whether to raise the security budget or insurance.

In other words, cyber risk may be increasing but at the same time the weapons to fight it are becoming more and more effective and more readily available.

For more information, contact:

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

Namrita Jhangiani
Mumbai
namrita.jhangiani@egonzehnder.com

Vineet Hemrajani
Mumbai
vineet.hemrajani@egonzehnder.com

Darpan Kalra
New Delhi
darpan.kalra@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. In addition, we have partnered with Paradox Strategies, co-founded by Harvard University Professor Linda Hill, to develop the Innovation Quotient (IQ), a proprietary culture diagnostic.

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, Twitter, and Instagram.