BoardMatters Forum

16 May 2024

Building a better working world

Key challenges, risks and responsibilities faced by Boards on cybersecurity and data privacy

The proliferation of new-age technologies such as IoT, Cloud and AI in business make cybersecurity and data privacy critical components of protecting sensitive information. Organizations are intensifying actions to safeguard the growing quantum of data generated and stored against increasingly sophisticated breaches and ensure continued trust of various stakeholders. Board overview can strengthen the defenses and support the organization in maintaining integrity and compliance.

EY hosted the Board Matters Forum (BMF) meeting on 16 May 2024, which included a panel discussion on 'Key challenges, risks and responsibilities faced by Boards on cybersecurity and data privacy'.

Burgess Cooper, Partner and Deputy Cybersecurity Leader, EY India moderated the panel. Its members were:

- Dr. Durga Prasad Dube, Executive VP and Head – IRM, Reliance Industries; member of Board level Standing Committee on Technology (SCOT) of Central Depository Services Ltd (CDSL); Chairman, SCOT of CVL (CDSL Ventures Ltd)
- Varun Singla, CISO, Airtel
- Vinay Deshpande, Head of Digital and IT, IHCL

Panel discussion

Balancing security with innovation

Today's fast-paced digital evolution is a double-edged sword. Organizations often prioritize rapid development and deployment over comprehensive security measures, especially in the early stages of their growth. This oversight can lead to vulnerabilities and exposure to cybercriminals. To effectively balance innovation with security, it is crucial to integrate robust security protocols from the outset and continually evolve them in tandem with technological advancements.

Attracting and retaining the right talent is part of the cybersecurity foundation. These professionals need challenging and engaging problems to solve, ensuring they remain invested in the organization's security posture. Managing the trade-off between innovative freedom and stringent security protocols is challenging, but essential. Maintaining stakeholder satisfaction is key to this equilibrium.

In industries like hospitality, digital transformation must go hand in hand with rigorous customer privacy management. A comprehensive approach would include a 24/7 incident security center, cyber defense, threat intelligence, encryption and privacy by design. Regular training and awareness programs that keep the workforce informed and vigilant are a basic yet effective component of defense. Compliance with domestic and international regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and India's Digital Personal Data Protection Act, 2023 (DPDP Act) further underscores the importance of a holistic approach where innovation and security complement each other to enhance customer experience.

Boards must ensure a proactive approach that enables blending innovation with security to protect both organizational and customer interests.

Role and responsibilities of CISOs toward the Board

The panel emphasized the need for Boards to develop a thorough understanding of the organization's assets and vulnerabilities. By posing questions to CISOs and assigning a chain of accountability, Board members can drive improvements in security practices.

CISOs have a crucial role in bridging the gap between cybersecurity and business innovation, especially in large organizations. A CISO's responsibilities include the implementation of encryption protocols, stringent access controls and supply chain optimization.

Regular cybersecurity assessments are essential to identify vulnerabilities and ensure that security practices evolve in line with technological advancements. By maintaining a robust and dynamic security posture, the CISO helps safeguard the organization's assets and customer data.

The CISO must also focus on fostering a well-informed and vigilant workforce. This involves conducting regular training sessions, launching awareness campaigns, and ensuring compliance with regulations. Such measures are integral to embedding a security-conscious culture within the organization.

By aligning security protocols with innovative business strategies, the CISO ensures that cybersecurity is not seen as a hindrance but as an enabler of growth and customer satisfaction. Through these efforts, the CISO plays a pivotal role in maintaining the organization's integrity and trustworthiness in an increasingly digital world.

A comprehensive view of an organization's cybersecurity framework means a CISO can effectively communicate the significance and scope of cybersecurity to the board, while also emphasizing the board's role in this direction.

Cyber resilience is the key

Boards must acknowledge the inevitability of cyber-attacks in today's landscape and shift the focus towards resilience and rapid recovery. This pragmatic approach emphasizes the importance of operational resilience and data protection as primary objectives for cybersecurity efforts. Understanding and articulating risk tolerance or risk resilience, rather than risk appetite, offers a more realistic framework for managing cybersecurity. This perspective recognizes that, while some risks can be mitigated, complete prevention is unattainable.

By prioritizing resilience, organizations can ensure they are prepared to respond effectively to breaches, minimizing downtime and maintaining critical operations. Implementing robust incident response plans, regular training, and continuous system monitoring are key strategies to enhance resilience. Ultimately, the goal is to create a security posture that not only defends against threats but also enables swift recovery, ensuring the organization can sustain its operations and protect its data.

Cybersecurity is the new-age equivalent to industry safety

The panel underscored the omnipresence of cybersecurity and the need to treat it as the modern equivalent of industry safety. Routinely addressing cybersecurity at every Board meeting can underscore its saliency and reinforce its critical role in the organization's overall strategy.

The panel also suggested a comprehensive approach, advocating an annual full-fledged presentation on cybersecurity complemented by regular overviews of security metrics in Board meetings. This will ensure that the Board remains informed and can make well-informed decisions.

The Board can drive measures that ensure the authenticity of information so that companies can address misinformation and disinformation proactively to safeguard the its resilience.

Companies should not view cybersecurity as an exceptional matter but as an integral part of daily operations. It requires continuous observation and management, much like any other critical incident. By embedding cybersecurity deeply into the organization's culture and routine practices, companies can better protect themselves and their stakeholders from evolving threats. A holistic approach ensures that cybersecurity is not just a parallel concern, but a central element of organizational resilience and operational integrity.

Other remarks

The efficacy of cybersecurity depends on good practices. Undergoing regular training on the latest developments will help Board members enhance their insight and address current issues. As new technologies emerge and pose new challenges, it is crucial for Board members to understand the roles and responsibilities of CISOs and CIOs, ensuring they are equipped to address these dynamic threats effectively.

Along with the right talent, budget allocation is also a part of an organization's cybersecurity and data protection foundation. External validations, red teaming exercises, third-party risk management, and supplier security assessments are equally important.

Board members can ask the right questions, thus fostering a proactive and informed dialogue. Coordination and collaboration among all stakeholders are necessary to strengthen the security posture collectively. This foundation allows for adaptation and resilience in the face of evolving threats, ensuring a secure organizational environment.

Our offices

Ahmedabad
22nd Floor, B Wing, Privilon
Ambli BRT Road,
Behind Iskcon Temple,
Off SG Highway
Ahmedabad - 380 059
Tel: + 91 79 6608 3800

Bengaluru
12th & 13th floor
"UB City", Canberra Block
No. 24, Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground & 1st Floor
11, 'A' wing
Divyasree Chambers
Langford Town
Bengaluru - 560 025
Tel: + 91 80 6727 5000

Bhubaneswar
8th Floor, O-Hub, Tower A
Chandaka SEZ, Bhubaneswar
Odisha – 751024
Tel: + 91 674 274 4490

Chandigarh
Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai
Tidel Park, 6th & 7th Floor
A Block, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR
Ground Floor
67, Institutional Area
Sector 44, Gurugram - 122 003
Haryana
Tel: +91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
Gautam Budh Nagar, U.P.
Noida - 201 304
Tel: + 91 120 671 7000

Hyderabad
THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jaipur
9th floor, Jewel of India
Horizon Tower, JLN Marg
Opp Jaipur Stock Exchange
Jaipur, Rajasthan - 302018

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

3rd Floor, Unit No 301
Building No. 1
Mindspace Airoli West (Gigaplex)
Located at Plot No. IT-5
MIDC Knowledge Corridor
Airoli (West)
Navi Mumbai - 400708
Tel: + 91 22 6192 0003

Pune
C-401, 4th Floor
Panchshil Tech Park, Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

10 Floor, Smartworks
M-Agile, Pan Card Club Road
Baner, Taluka Haveli
Pune - 411 045
Tel: + 91 20 4912 6800

Ernst & Young LLP

EY | Building a better working world

About EY

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram - 122 003, Haryana, India.

EYIN2406-013
ED None

SJ