Cyber risks – A persistent threat for boards

Cyber Risk Management has transitioned into a key strategic consideration for Boards rather than simply being an operational risk consideration as in the past.

With the emergence of an inter-connected data-driven corporate world reliant on sanctity of systems and networks for income and productivity, Cyber risk has risen steadily to the ranks of top risks for Directors and Officers (D&O) today.

According to the 'Global D&O Liability Survey 2021' conducted by Willis Towers Watson in conjunction with global law firm Clyde & Co, 'Cyber Attacks' and 'Data Loss' were voted as the top two D&O concerns. Cyber-attacks and Data loss have featured in the top 3 risks overall since 2016 and 2021 saw no difference: 56% and 49% of the global respondents voted for 'Cyber Attack' and 'Data Loss' respectively as being the top concerns for the year as per the report.

Key concerns amongst the D&O are related to the financial, reputational, regulatory and operational implications of cyber breach incidents. Abundant cyber loss statistics and recent regulatory actions resulting in multimillion-dollar fines in recent times have attracted heightened concerns amongst the CXO community.

Having witnessed the devastating impact of cyber-attacks, governments are formulating regulations that impart greater responsibility on Boards in managing cyber risks. There seems to be a two-pronged approach in the action plans of global data privacy regulations and governmental reforms around cyber security guidelines. Firstly, regulators are establishing Board responsibility in ensuring the security of the Information assets of the company through adoption of broad Cyber security and Information Security Management systems which need to be reviewed periodically. Secondly, regulators are expecting the Boards to personally sign off and be accountable for the overall information security management systems including the delegation process, elements associated with incident response and reporting of incidents.

Information Security Management Frameworks like ISO 27001:2013, NIST CSF etc. widely establish the crucial responsibility of top management in establishing processes and systems that ensure the confidentiality, integrity and availability of data. Emerging legislation and cyber risk management frameworks suggest that the scale of expectations placed on directors to promote cyber resilience will only increase in the future.

Data privacy law reforms recently implemented or on the agenda in APAC jurisdictions such as Japan, Singapore, Australia, New Zealand and India are giving individuals a greater right to privacy in terms of how their personal and sensitive information is handled and enabling direct actions against companies mishandling their data. This indicates that the historical perception of a 'relaxed' regulatory environment and the culture in APAC region will see a tremendous shift in the coming years with the reformatory legislations by various governments in the region in the data protection environment.

COVID-19 provided the perfect conditions for hacking communities to exploit the unplanned proliferation of technology and infrastructure galvanised by the remote working arrangements across the globe by exponentially widening the cyber attack surface area. The exponential rise in ransomware activity (for example, the Colonial Pipeline attack) coupled with supply chain risks created by cyber-attacks on the technology and

managed service provider's systems during 2020 and 2021 (for example, the Kaseya cyber-attack) have demonstrated the complex and dynamic nature of the cyber risk environment organisations are grappling with today.

Drawing from the above events, Boards also need to be wary of the increased proximity to class action suits either from shareholders affected by the reputational impact or from the group of affected individuals empowered by the reforms in data privacy laws holding the Board members personally liable for failure of duty to safeguard customer information. Such events can also trigger an organisation's notice obligations under contract or under multi-jurisdictional and/or international breach notification laws.

The uptick in cyber events in 2020 and 2021 have proven beyond point for D&Os that cyber and data security related issues will continue to be a persistent threat and thereby D&Os need to be constantly and proactively involved in adopting a holistic cyber risk management approach which spans across the people, process and technology. Since the threat is real and imminent, in addition to continued investment into IT security, Boards need to actively consider a financial recovery plan for when crisis strikes, through a consultative approach to quantifying loss potentials and adopting appropriate and optimum risk transfer mechanism such as Cyber risk insurance.

This article was first published in CIOL.

About the Authors:

Jennifer Tiang
Regional Cyber Lead, Asia
Willis Towers Watson
Jennifer.Tiang@willistowerswatson.com

Suraj Theruvath
Vice-President – Financial and Executive Risks
Willis Towers Watson India Insurance Brokers
Suraj.Theruvath@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.