Risk transfer considerations for critical infrastructure in India

The Critical Infrastructure (CI) of a country consists of all the organisations, systems, networks, assets, and services that are essential for its security and economic wellbeing. Disruptions to CI could have wide-scale implications on the affairs of a country. Consistent with wider industry, CI entities have undergone significant levels of digitisation in the recent times with the advent of IT (Information Technology), OT (Operational Technology) and Industrial Internet of Things (IIoT) technologies automating most of the production and business functions.

Owing to their geographic and economic criticality for respective nations, rich cash reserves and their increasing reliance on systems and networks, CI companies have in recent times been targeted by malicious cyber threat actors with diversified intent ranging from state sponsored terrorism, data theft, holding victims to ransom, and causing disruption for purely criminal financial gain.

Indian CI has been under constant threat and attack by state and non-state actors. As per reports, the advanced cyber-attack on Pune based Cosmos Bank in 2018 reportedly saw INR 94.4 Crores siphoned to offshore bank accounts, hackers gaining access to government's UIDAI data of 1.1 billion users, hacking attempt on ISRO's databases during the launch of Chandrayan-2 mission, hackers stealing information from India's Kudankulam Nuclear Power Plant and more recently, the cyber hacking attempt on Mumbai's Power Grid are testament to the growing menace of cyber risks facing Indian CI. Power and energy sector companies have been the most targeted while other CI establishments have been intermittently targeted.

While IT systems have traditionally been under the radar, hacking groups have recently shifted focus on more valuable and often vulnerable OT systems as a more lucrative option from an economic and impact standpoint.

OT Systems were traditionally not built with security in mind, largely operating in closed and highly segmented environments and thereby discounted from security considerations owing to their remoteness from network connections. With the emergence of IT and OT inter-connectivity, distributed Industrial Control Systems, IIoT systems and migration to cloud systems through third party service providers, enterprising threat actors can cause mayhem in the form of Distributed Denial of Service attacks. They manage to do this by entering laterally through interconnected systems, hijacking and manipulating IIoT systems causing equipment malfunctions. This results in property damage, resultant bodily injury and in some cases environmental pollution situations. Business interruption and supply chain losses in such instances can quickly escalate to cause multi-million losses for victims. Ironically, in many instances witnessed across the globe, hackers have only had to threaten the dire consequences to successfully extort ransom monies from targeted victims.

Economical risk transfer considerations amidst digital security transformation

While technical defense is bound to enhance over time, CI owners need to acknowledge that the threat actors are constantly improving their exploits. This indicates that a cyber-attack on a previously unseen vulnerability (zero-day vulnerability) is quite probable. This necessitates investments into loss quantification studies where both IT and OT environment owners need to have equal participation to understand the prospects of a cyber incident on the organisation's balance sheet.

Analytical projections associated with Loss of productivity/ income, the incident response costs, civil liabilities and any applicable regulatory implications in the form of legal representation costs and any fines and penalty projections must be obtained through external consultants.

Loss potentials mentioned above falling beyond risk appetites can be transferred onto a Cyber Risk Insurance which is gaining relevance across the globe. While historically the level of take-up in India has been relatively low, there has been a steady rise in the last 18 months.

Cyber insurers are now judiciously offering additional covers for property damage, bodily injury, IT assets reconstitution (Bricking costs), failure to supply contractual liabilities, voluntary/ governmental shutdown, business interruption losses etc.

Risk Management Value proposition from Insurance

CI owners can derive significant value from cyber insurance application and the underwriting process. Insurers are increasingly relying upon in-house/ collaborative cutting-edge cyber risk assessment technologies coupled with detailed questionnaires consisting of relevant questions for holistically assessing the applicant's cyber risk maturity. Based on the responses and findings, insurers along with brokers can provide an in-depth opinion about an organisation's current risk posture and advise on areas on improvements. This is largely derived from the global loss experience of Insurers/ Reinsurers/ Brokers and from their peer group and industry, providing the top management comprehensive external opinion. Such evaluations are conducted periodically through regular assessment reports and annual renewal exercises forming a collaborative and consultative risk identification, analysis, and treatment alliance with insurer/ broker.

A holistic approach involving cyber awareness trainings, process improvements, implementing industry standard frameworks (NIST CSF, PERA Model, ISA/IEC 62443 etc.) is the need of the hour. Industry collaboration for incident response and reporting along with consideration of an optimum cyber risk insurance based on cyber risk assessment and loss quantification studies can help CI institutions to be better prepared, respond and recover financially from evolving and persistent cyber incidents.

This article was first published in EPC World.

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.

Copyright © 2021 Willis Towers Watson. All rights reserved
willistowerswatson.com