Dealing with ransomware

One year on from COVID-19 being declared a global pandemic, we are also living in the aftermath of what can be described as the world's largest en-masse digital transformation project. The confluence of remote working together with the rise in sophistication of organised cyber-criminal groups has led to the rise of Ransomware as one of the most significant cyber risks to face organisations and governments alike.

Ransomware is a malware or malicious software that accesses vulnerable files and systems and locks the users out by encrypting the files or systems until a ransom money is paid by the victim to obtain decryption key.

Over the years various state sponsored/independent cyber-criminal outfits like 'Ryuk', 'REvil', and 'Darkside' have emerged and developed a highly lucrative business model known as 'Ransomware as a Service (RaaS)' where ransomware developers form alliances with other cyber-criminal groups ('Affiliates') who increase their outreach and share the proceeds of exploits in pre-agreed proportions.

Supply chain risks have emerged as a significant threat vector where a threat actor infiltrates the system through third party service providers. The recent case of a ransomware attack impacting roughly 1,500 downstream customers of Managed Service Providers (MSPs) demonstrates the borderless and far reaching impact of ransomware attacks.

Financial Impact

According to Willis Towers Watson's (WTW's) Global Cyber Insurance Claims data, the average ransomware demand in 2020 was between $4-4.5 million (up from under $3.5 million in 2017), with the average ransom payment noted as slightly above $1.6 million. According to Sophos's 'State of Ransomware 2020' report, India is statistically the most impacted, with average ransomware remediation costs of $1.1 million and average ransom payment being $76,619.

The size of ransom demands has been dominating cyber headlines in recent times. As per media reports, insurer CNA Hardy allegedly paid USD 40 Million; and ransomware demand associated with Kaseya reportedly being USD 50 Million. However, the business and financial impact of a ransomware attack is complex and multifaceted. Many technology companies in India could also be exposed to significant fines and penalties for breach of privacy laws emanating from a ransomware related data breach incident.

Furthermore, unavailability of systems can lead to significant loss of revenues depending on a company's operating and revenue model. Business interruption losses can escalate further by additional operational expenses incurred for alternate arrangements to maintain productivity during unavailability of systems and networks.

IT Forensics, Data Reconstitution and other Crisis Management expenses also add up significantly depending on the number of systems, networks to be remediated.

Business leaders must focus on 'Resilience' by adopting a holistic, cross-functional approach to assessing and quantifying cyber risks. Organisations must invest in developing a cyber-savvy culture through regular enterprise-wide anti-phishing and social engineering trainings and ongoing communications reminding employees to be vigilant about suspicious online activity.

Ransomware response strategies must be embedded in Information Security Management Systems (ISMS), Business Continuity Plans (BCP), Incident Response Plans (IRP) and Data Back-up processes which are to be tested periodically for efficacy with clear decision-making rights established and delegated in the IRP.

Cyber loss quantification studies can help risk managers to understand loss potentials and adopt optimum risk transfer mechanisms such as Cyber Risk Insurance to not only transfer the pecuniary impact but also to augment their incident response strategies through collaborations with the insurer. Industry collaborations can help in exchange of learnings and cyber risk trends for the benefit of the participating organisations.

Ransomware risk has become more imminent than probable and so a holistic approach which spans across people, process, and technology coupled with periodic risk assessments and risk transfer strategies is called for. Working with the right advisory partners can help organisations understand their risks, improve their defense and obtaining adequate insurance can then reduce the overall financial impact in the event crisis strikes.

This article was first published in Hindu BusinessLine.

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.