TATA CONSULTANCY SERVICES

Building on belief

Ecosystems:

The path to combating cyber risk

Abstract

The risk of cyberattacks and consequent losses is on the rise as almost every business adapts to a digital model. With the rising incidence of sophisticated cyber-attacks such as the Solarwinds[1] supply chain attack and the more recent Verkada[2] security camera hack, the need for cyber insurance has never been greater. Enterprises must opt for cyber insurance to protect digital assets including customer data and build resilience against cyber risks. However, insurers neither have sufficient loss data to model risks confidently and offer protection nor the expertise to identify and mitigate constantly evolving cyber risks. As a result, they have not been able to meet the market demand. The way forward is to understand customers' security needs and leverage an ecosystem of cybersecurity partners offering risk assessment and prevention, post-breach recovery management, and loss mitigation services. This white paper highlights the importance of the service provider ecosystem in building cyber resilience and growing cyber insurance portfolios with prevention at the core.

Cyber insurance: Closing the gap in the cyber armory

With more and more organizations treading the digital path the cyberattack surface has expanded and exposed them to cyber risks and increasing threats of an attack. Additionally, post the pandemic outbreak, work-from-home has become the norm and many organizations have transitioned to the cloud to ensure continued smooth operations. However, most firms in the small and medium enterprise (SME) segment lack an understanding of their risk exposure and the damage it can cause to their business. This lack of awareness and absence of resources or measures to fight cyber risk further exacerbates the potential dangers. The severity of a cybersecurity incident and the widespread damage it can cause cannot be underestimated, and cyber insurance coverage thus becomes crucial.

Cybersecurity insurance provides coverage for compromised security or data breach. It also covers investigation costs, financial losses due to downtime or inability to recover data, third-party notification costs, and legal expenses post a cyber-attack. For insurers, offering risk and loss mitigation services along with cyber protection is fast emerging as a key differentiator. However, many insurers may lack the necessary expertise to accomplish this. With regulations such as the IoT Cybersecurity Improvement Act being introduced, insurers must consider leveraging the cyber insurance partner ecosystem to ensure regulatory compliance as well as strengthen customers' cybersecurity preparedness.

---

[1] Reuters, IT company SolarWinds says it may have been hit in 'highly sophisticated' hack, December 2020, Accessed April 2021, https://www.reuters.com/article/us-usa-solarwinds-cyber-idUSKBN28N0Y7

[2] Bloomberg, Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals, March 2021, Accessed April 2021, https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams

Leveraging the services of partner firms will help insurers grow their cyber insurance portfolio and improve customer experience over the long-term backed by the ability to better manage exposure and detect new risks. An ecosystem model enables insurers help customers improve cyber resilience and define an appropriate strategy by leveraging artificial intelligence (AI) and machine learning (ML) technologies for quick breach identification and response. Forging partnerships with cybersecurity players will help insurers understand customers' cybersecurity landscape and improve their cyber posture.

Leveraging the cyber insurance ecosystem

Unlike other mature lines of business (LoBs) like automobile and property, cyber risk data is not readily available due to its sensitivity. The absence of historical cyber insurance data and uncertain risk scenarios coupled with the evolving nature and increasing sophistication of cyberattacks add to the challenges in pricing cyber insurance products. Insurers tend to address these challenges by limiting or excluding coverage for uncertain risks. Consequently, customers stop seeing value in limited coverage policies and instead invest in cybersecurity measures. The result is low market penetration of cyber insurance widening the gap between demand and supply of cyber coverage.

To be profitable in the long-term and sustainably grow their cybersecurity portfolio, insurers must manage risk exposures, detect new risks, ensure customers have a proper breach response strategy, and enhance coverage by introducing risk mitigation measures. To accomplish this, insurers must partner with players that can adapt and scale to offer services (see Figure 1) such as cybersecurity posture assessment, cyber education for customers, risk prevention, and post breach notification and loss mitigation. This improves the insurability of previously uninsurable risks and mitigates the extent of cyber incident claims.

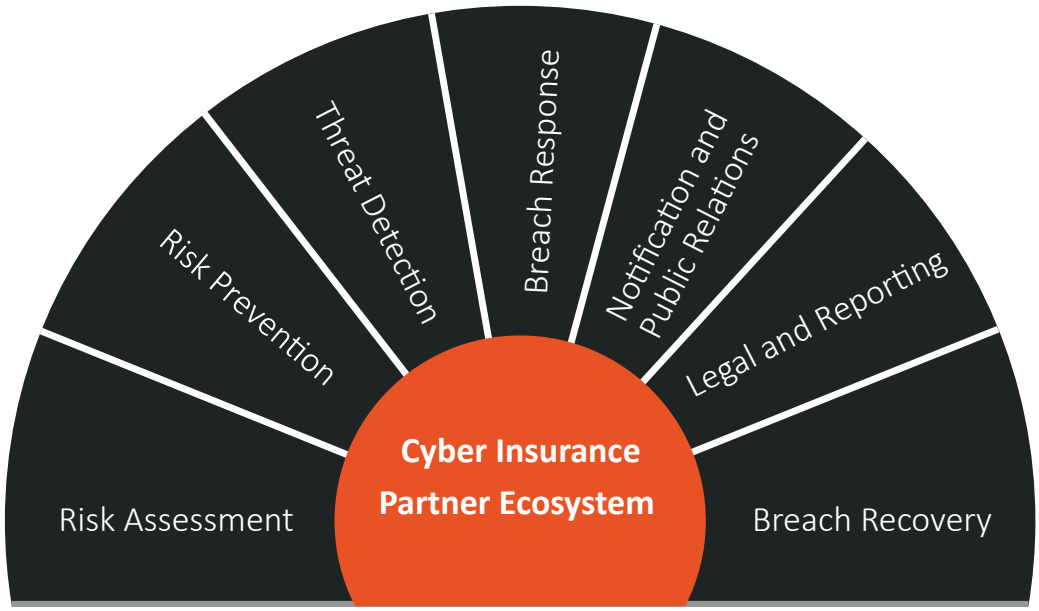

Figure 1: Cyber Player Ecosystem and Services Offered

Such a partnership approach can also present opportunities for insurers to recommend appropriate services offered by these partners to their customers creating a whole new value ecosystem.

Risk assessment

Determining the insurability of risks is a crucial first step before insurers can underwrite it. However, insurers face challenges due to lack of cyber incidents data and knowledge of advanced threats and the absence of modeling frameworks to assess risks. Building risk assessment capabilities in collaboration with ecosystem partners can help insurers ascertain the risk posture of organizations. Ecosystem players can help evaluate systems, applications, and processes to identify vulnerabilities and arrive at evidence-based cybersecurity ratings. Insurers can also leverage their services and use the ratings to determine the insurability of risks and aid underwriting decisions. In addition, these assessments help ensure affordable premiums, especially given that the average loss ratio rose to 44.9% in 2019 from 35.4% in 2018.[3]

Risk prevention

Most insurers offer post-breach assistance; however, it is crucial to understand and prevent risk. Risk prevention services range from vulnerability or compromise assessment to employee education, and building cybersecurity incident awareness. They provide continuous end-to-end monitoring, endpoint detection, identity theft, credit monitoring and regulatory non-compliance. Insurers must impress on their customers to implement risk prevention strategies as it helps to provide better coverage at lower premiums. By enforcing these measures, insurers can increase employee awareness and reduce the risk of ransomware attacks and phishing attempts. This will help insurers lower claims losses and offer better premiums to customers, which is mutually beneficial.

Threat detection

Proactive threat detection and attack prevention demand threat intelligence and threat hunting for real-time detection of malicious activity. Insurers must incentivize customers to adopt threat detection mechanisms that thwart cyber-attacks at the perimeter and isolate the asset to prevent further damage. Insurers must partner with service providers that leverage AI and ML technologies to offer real-time threat intelligence and actionable insights.

Breach response

Speed of response to cyber-attacks largely determines the potential damage. A well-defined incident response strategy is key to mitigate the impact of a breach. When an incident occurs, customers look for quick access to an expert panel for forensic investigation, notification, fraud consultation, and identity restoration services. Partnering with ecosystem players can help insurers offer these services and reduce business interruption claims.

Notification

Once a breach is detected, the insured party needs to notify several stakeholders as per jurisdiction-specific regulations. By partnering in this space, insurers can offer direct assistance to meet notification commitments, provide call center services, and handle public relations queries. Timely reporting is essential for compliance with data privacy laws, which requires communication within 24 hours to avoid hefty penalties. This helps customers prevent reputational damage and avoid penalties, which are claimed as part of first party coverages.

---

[3] Reinsurance News, US cyber insurance market's loss ratio up 10% on claims frequency: Aon, June 2020, Accessed May 2021, https://www.reinsurancene.ws/us-cyber-insurance-markets-loss-ratio-up-10-on-claims-frequency-aon/

Legal and reporting

Several large breaches have triggered lawsuits resulting in massive punitive penalties[4] and reputation loss. Post a breach, organizations need legal services to help determine the immediate steps to comply with applicable breach notice laws and contain the damage in turn limiting claims for the insurer. Legal firms in the ecosystem provide counseling and litigation services as well as advice on compliance issues related with regulations such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA). Insurers must recommend their services to customers to ensure regulatory compliance and reduce the impact of a cyber event.

Breach containment and recovery

Containing a data breach by preventing unauthorized access and removing intruders is vital to defend against claims-related litigation due to negligence on the part of the insured. Speed of detection, containment, and remediation are critical factors in mitigating losses for insurers. Ecosystem players offer recovery services for cybercrimes such as breach of personal data and intellectual property and minimize business interruption.

In a nutshell

Insurers venturing into cyber insurance without the necessary expertise, may see growth in the short term due to initial demand. However, they are likely to incur a significant loss in the event of a systemic risk. Carriers typically resort to reinsurance to transfer this risk rather than build the necessary expertise to overcome it, which has slowed the adoption of ecosystem models often leading to capacity challenges. However, considering cybersecurity is a niche area and needs specialized expertise, insurers must leverage ecosystems and bring in partners with the requisite know-how and proficiency. Collaboration will eventually strengthen the cybersecurity ecosystem and drive the market toward exponential growth through increased customer adoption of cyber insurance.

About the authors

Nirmal Kumar J

Nirmal Kumar J is a solution architect with the Banking, Financial Services, and Insurance (BFSI) business unit at TCS. He has over 18 years of experience in the insurance Industry and has worked with leading insurers on transformation programs. He specializes in development of IT solutions, especially BPM solutions for clients. He holds a Bachelor's degree in Computer Science and Engineering from the University of Madras, India.

Amarnath Suggu

Amarnath Suggu is a senior consultant with the Banking, Financial Services, and Insurance (BFSI) business unit at TCS. He has more than two decades of experience in the insurance industry, predominantly with property and casualty (P&C) insurers. His areas of interest include emerging technologies, especially artificial intelligence and its numerous applications in the insurance industry. He holds a Master's degree in engineering from the Indian Institute of Technology, Chennai, India.

---

[4] Attorney General of Washington, EQUIFAX TO PAY UP TO $700M FOLLOWING AG INVESTIGATION, July 2019, Accessed May 2021, https://www.atg.wa.gov/news/news-releases/equifax-pay-700m-following-ag-investigation

Awards and accolades

Contact

For more information on TCS' Banking, Financial Services, and Insurance (BFSI) unit, https://www.tcs.com/banking-financial-services or https://www.tcs.com/insurance

Email: bfsi.marketing@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 488,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS_News**.

All content/information present here is the exclusive property of Tata Consultancy Services Limited (TCS). The content/information contained here is correct at the time of publishing. No material from here may be copied, modified, reproduced, republished, uploaded, transmitted, posted or distributed in any form without prior written permission from TCS. Unauthorized use of the content/information appearing here may violate copyright, trademark and other applicable laws, and could result in criminal or civil penalties.

Copyright © 2021 Tata Consultancy Services Limited

Corporate Marketing | Design Services | M | 08 | 21