Decoding the Secrets of Cyberinsurance Contracts

Cyberattacks are emerging faster than ever in the wake of the COVID-19 pandemic. As new dimensions are incorporated into these disruptive cyberattacks, enterprises around the world must be more vigilant about protecting their critical information assets. Chief information security officers (CISOs), chief information officers (CIOs) and chief executive officers (CEOs) are continually working to identify more effective ways to prevent their enterprises from falling victim to these dynamic threats. By the end of 2020, global cybersecurity and cyberinsurance spending was projected to reach US$124 billion.[1] Cyberinsurance has become an important element of the loss recovery measures instituted after a cyberattack. It covers the potential financial losses caused by cyberattacks and the costs of digital forensic investigations and lawsuits following an attack.

Blanket Bond Insurance Contracts

In general, enterprises purchase blanket bond insurance contracts to cover potential losses caused by any man-made or natural disasters. **Figure 1** lists the various losses covered (and not covered) by blanket bond insurance contracts based on comparative analysis of cyberinsurance offerings from various insurance firms offering cyberinsurance contracts against blanket bond insurance contracts of sampled organizations.

Figure 1 illustrates the gaps between blanket bond insurance contracts, which provide only partial protection against cyberattacks, and exclusive cyberinsurance liability contracts, which are becoming popular. There are two options to address these gaps: enterprises can ask their current insurers to enter into coinsurance or reinsurance arrangements with cyberinsurance providers to get complete protection from cyberattacks, or they can buy exclusive cyberinsurance contracts from niche cyberinsurance enterprises in the marketplace.

Cyberinsurance Contracts

Even exclusive cyberinsurance contracts have some restrictions on the types of coverage provided. For example, the following losses are not covered by cyberinsurance contracts:

- Loss and damage from unfair trade practices; employment practices; willful, intentional, deliberate, malicious, fraudulent, dishonest or criminal acts; breach of contract; or theft of trade secrets committed by the insured or by third parties (i.e., suppliers, partners, service providers) working with the enterprise
- Business losses during unexpected downtime caused by cyberattacks

Vimal Mani, CISA, CISM, Six Sigma Black Belt
Is head of the Information Security Department of the Bank of Sharjah. He is responsible for the bank's end-to-end cybersecurity program, coordinating its cybersecurity efforts across the Middle East; implementing its cybersecurity strategy and standards; leading periodic security risk assessments, incident investigations and resolution efforts; and coordinating the bank's security awareness and training programs. He is an active member of the ISACA® Dubai Chapter. He can be reached at vimal.consultant@gmail.com.

Figure 1—Losses Covered by Blanket Bond Insurance Contracts

Losses Generally Covered
• Loss of property from premises due to theft, burglary, robbery and purposeful attacks • Loss caused by dishonest or fraudulent acts committed by employees • Loss of property in transit • Loss of or damage to offices and their contents, such as furniture and equipment (including all kinds of information assets), caused by burglary, robbery, theft and any other illegal act • Loss of and damage to electronic data media caused by robbery, burglary, theft, malicious damage, misplacement or disappearance due to unknown reasons • Loss of and damage to data due to virus attacks • Loss of and damage to data due to physical attack or intrusion • Interception of communications sent and commission of fraud by using the same • Loss and damage caused by forged signatures • Loss and damage caused by forged fax messages • Loss of and damage to computer programs • Loss of and damage to data stored in electronic media • Loss of and damage to data processing media such as magnetic tapes, magnetic disks and other bulk media • Loss and damage caused by commotion, riots, hostilities, rebellion, revolution or warlike operations • Loss and damage caused by radiation, explosions, and toxic and hazardous materials • Loss and damage caused by threats made with the intention to harm a person or physical premises • Loss and damage caused by loss of mail transported in nonarmored enterprise vehicles • Loss of and damage to the premises caused by mechanical failure, faulty construction, wear and tear, electrical disturbance, electronic media processing failure, and failure of software programs
Losses Not Generally Covered
• Loss and damage caused by social engineering attacks via telephone, fax or email • Loss and damage due to data privacy breaches (unauthorized access to data resulting in customers' private data reaching unauthorized hands) • Loss and damage due to fraudulent or defective computer programs procured by the enterprise • Loss and damage caused by the purposeful commission of fraud through the misuse of access privileges (e.g., accessing a critical system to steal data) • Loss and damage from network failure due to cyberattack • Loss and damage (reputational and financial) due to the threat of intentional cyberattack by an outsider attempting to extort money, securities or other valuables • Loss and damage due to online defamation via social media • Loss and damage due to ransomware attack (request for ransom by adversaries)

- Loss of intellectual property (e.g., source code, product designs)
- Loss and damage due to data encryption failure
- Costs related to software upgrades and hardware replacement
- Costs to improve the enterprise's cybersecurity infrastructure
- Costs related to breach of contractual liabilities by the insured
- Costs related to fines imposed by law enforcement agencies or regulators for crimes committed, policy violations and noncompliance issues
- Injuries to personnel and property damage
- Loss and damage due to acts of foreign governments
- Loss and damage due to violations of consumer protection laws by the insured
- Loss and damage due to online defamation via social media

Figure 2 describes the types of cyberinsurance contracts being sold in the marketplace. Before purchasing cyberinsurance, enterprises should take the following steps:

- Perform a detailed cyberrisk assessment with the help of an expert from the industry and identify the current cyberthreat landscape.
- Review the existing blanket bond insurance contract for any gaps in coverage for the cyberrisk factors identified during the cyberrisk assessment.

Figure 2—Types of Cyberinsurance Contracts

First-Party Cyberinsurance Contracts	Third-Party Cyberinsurance Contracts
• Provides coverage against losses incurred directly by the insured enterprise • Provides coverage against losses due to damage to critical information elements, software and systems of the insured enterprise • Provides coverage for revenue losses caused by network security breaches or failures • Provides coverage for losses arising from the theft or fraudulent use of the insured enterprise's data and critical information systems by adversaries • Provides coverage for ransomware threats from adversaries of the insured enterprise • Provides coverage for the cost of forensic investigations conducted as part of the incident response cycle	• Provides coverage against claims for losses incurred by third-party enterprises or individuals (suppliers, partners, service providers) working with the insured enterprise • Provides coverage against losses due to the theft or misuse of data held by third-party enterprises or individuals (suppliers, partners, service providers) working with the insured enterprise • Provides coverage for network liability (downstream), protecting against distributed denial-of-service (DDoS) and bot attacks against third-party enterprises or individuals (suppliers, partners, service providers) working with the insured enterprise • Provides coverage against liability (lawsuits and resulting judgments) for losses of third parties (suppliers, partners, service providers) arising from the negligence of the insured enterprise

- Discuss with the existing insurer the possibility of enhancing the existing contract to include coverage of identified cyberrisk factors.
- If the insurer is not in a position to revise the existing blanket bond insurance contract, search the marketplace for niche insurers and insurance brokers in the industry offering exclusive cyberinsurance plans.
- Evaluate the cybersecurity and data privacy practices of all potential insurers or insurance brokers and identify the most reputable ones. This is very important because enterprises share significant amounts of business-related information with these insurers.
- Discuss with the selected insurers which cyberthreats should be covered by the cyberinsurance plan. Carefully review the plan provided by insurance underwriters for any gaps and misinterpretations. For example, time is critical in ensuring that coverage is triggered appropriately. A policy requiring that a "claim" be made before coverage applies may not be in line with the enterprise's expectations. Instead, a policy that is triggered upon the "discovery" of a data breach may be more appropriate. Likewise, legal liabilities may be unclear in the plan document. Because insurers are often required to pay out only what is legally required, an enterprise may be liable for outstanding damages that are not covered by insurance. All plan agreements must be carefully read and vetted by the enterprise's legal counsel.
- Review the details of first- and third-party coverage as coverage limitations may differ from insurer to insurer. Review the plan and negotiate for more coverage if it is deemed inadequate to cover costs payable.
- Review the liabilities section of the plan document carefully. In general, the third-party liabilities section should cover the insured for liability arising from cyberattacks.
- Review exclusions mentioned in the plan documents and negotiate to limit exclusions as much as possible.
- Review the scope of services offered by the insurer as part of the plan.
- Request the removal of sublimits from the policy. If they cannot be removed, negotiate the highest sublimit possible for the lowest cost.

Figure 3 shows the types of protection offered by cyberinsurance products currently sold in the marketplace.

Conclusion

To survive and thrive in the increasingly complex cyberthreat landscape, enterprises should consider cyberinsurance plans. The benefits of these plans extend far beyond mere reimbursement of financial losses. Cyberinsurance plans are evolving into products that help insured enterprises assess their cybersecurity posture and strengthen their incident response capabilities. Cyberinsurance plans are an

Figure 3—Cyberinsurance Offerings

Main Offerings

- **Fines and investigations**—Covers the potentially significant costs of data protection regulator investigations and legally insurable fines following data security breaches
- **Crisis management**—Covers cyberincident response services following a data breach, public relations services to repair enterprise and individual reputations, breach coaching and notification, and monitoring of costs associated with a breach
- **Electronic data protection**—Covers the costs of making data safe again after a leak or a breach including third-party loss, first-party loss, lost income and additional operating expenses incurred
- **Security and privacy liability**—Covers third-party claims arising from a failure of the insured's network security or a failure to protect personally identifiable information (PII) and responds to regulatory actions connected with a security failure, privacy breach, or failure to disclose a security failure or privacy breach
- **Event management**—Covers security failures or privacy breaches, including the cost of notifications (including voluntary notifications), public relations, and other services to manage and mitigate a cyberincident, forensic investigations, legal consultations and identity monitoring for victims of a breach
- **Business network interruption**—Covers loss of income and operating expenses when business operations are interrupted or suspended due to a network security failure
- **Cyberextortion**—Covers the threat of intentional cyberattacks by an outsider attempting to extort money, securities or other valuables and includes the cost of an investigation to determine the origin of the threat
- **Damages due to online defamation**—Covers loss of reputation and subsequent financial loss due to online defamation via social media
- **Copyright and trademark infringement**—Covers losses due to any infringement of copyrights and trademarks owned by the insured

Additional Offerings

- Provision of cyberrisk intelligence
- Free infrastructure vulnerability analysis
- Access to risk management tools
- Proactive shunning service (protection measure to avoid hackers)
- Legal consultation on cyberrisk
- Investigation of cyberincidents by an expert team
- Free cybersecurity maturity assessment enabled by niche tools
- Complimentary security rating report to measure the enterprise's security performance

effective way to build a strong cyberresilience capability. With the arrival of the Fourth Industrial Revolution and significant developments driven by digital technologies such as fintech, blockchain, robotic process automation (RPA) and the Internet of Things (IoT), the possible cyberattack vectors are increasing. Purchasing suitable cyberinsurance plans will help enterprises transfer the responsibility for mitigating these cyberrisk factors to insurers.

Endnotes

1 Clement, J.; "Global Cyber Security and Cyber Insurance Spending 2015-2020," Statista, 10 November 2020, *https://www.statista.com/statistics/387868/it-cyber-security-budget/*