COVID - 19 and the threat to Cyber Security

In the wake of COVID-19 pandemic, the global economy is facing a potential meltdown. Like other countries, India has also gone into a country-wide lockdown to contain the spread. Companies are trying to cope with this new daily reality that now includes working from home, extensive use of digital platform for all ongoing statutory and regulatory compliance matters, and embracing digitisation to the best extent possible. New measures may usher in new risks. Enhanced digitisation is likely to increase cyber and data risk exposure of a corporation.

Cyber Security threats stemming from the Covid-19 chaos

The spread of the Covid-19 has changed the way we work. The Central and State Governments have directed private organisations to keep their offices shut and allow work from home where possible, making them vulnerable to cybersecurity threats. Scammers are taking advantage of the situation, by sending emails and text messages that appear to be sent from the government and health ministries, but are click baits used to hack into computer systems and steal sensitive information critical to individuals and organisations.

Use of digital platforms is being encouraged by public and private players alike. Frequent messages are being received from insurance companies and telecom companies, with banks imploring the public not to visit their branches / offices, and instead use online media for all services. Insurance Regulatory and Development Authority of India ("IRDAI") too has released circulars encouraging insurance companies to make special efforts to enable policyholders to pay premium using digital methods by educating them through SMS, emails etc., and has directed policy documents be issued through email, where available, within the prescribed period. SMS may also be used to confirm to the policyholders about issuance of policy documents. Insurers are encouraged to capture email and phone number of prospective customers for intimation of commencement of the policy and for further policy servicing.

Increased activity in the virtual medium is likely to come with its set of risks and make servers susceptible to attack by hackers. One such example is Business Email Compromise (BEC) attack mentioning coronavirus reported by Agari Cyber Intelligence Division (ACID). The attack, a continuation of an earlier BEC campaign, came from Ancient Tortoise, a cybercrime group behind multiple BEC cases in the past. Hackers first target accounts receivable into forwarding aging reports (accounts receivable reports). Then, while posing as legitimate companies, they use customer information in these reports to send emails to inform customers of change in bank and payment methods due to COVID-19. In another instance, a scammer sending an e-mail that appears to be sent from "GOV" shares a link to help people find out where they can get tested for coronavirus. These are click-baits which upon accessing may install malware on the computer and lead to stealing personal sensitive information including banking information or other company information.

Cyber and Data Security Policy

A cyber and data security insurance policy is designed to safeguard businesses from the potential effects of cyberattacks, procured by organisations to mitigate risk exposure by offsetting costs after a cyber attack/breach, designed to cover fees, expenses and legal costs associated with cyber breaches after an organisation has been hacked or from theft or loss of client/employee information.

What role does your insurance policy play in such situations?

The primary purpose of availing cyber data and security policy is to cover losses and liabilities arising out of data and privacy breach, network security breach, financial loss due to cyber theft, etc.

Typically, a cyber policy aims to indemnify for data-related loss and not physical loss. A standard Cyber Security Policy would cover

1. Cost to replace or restore electronic data or programs damaged, destroyed or stolen in a data breach
2. Cost and expenses incurred as a result of such data breach
3. Cyber extortion
4. Notification / defines costs.

The liability coverages afforded by a cyber policy are usually claims-made.

Coverage would usually also apply to damages or settlements that result from covered claims as well as the cost of defense.

What should organisations do?

Organisations ought to put suitable mechanisms in place to ensure safety firewalls for computers are secure enough to prevent any breach of data. It is becoming difficult to prove a direct loss that triggers a claim under the insurance policy if the insured fails to put in place safety mechanisms to curtail risks. Sufficient information at all levels of the organization about the risks of social engineering and common scams like phishing emails and typosquatting should be provided. The organisation must invest in tools that limit information loss, monitor third-party risk and fourth-party vendor risk, and continuously scan for data exposure and leak credentials. The use of technology to reduce costs like automatically sending out vendor assessment questionnaires as part of an overall cyber security risk assessment strategy must be encouraged. There should be real time assessment to ensure safety standards are being maintained by all employees in order to track leak/ loss of information promptly.

Earlier this week, the IRDAI issued a circular acknowledging the potential for an increase in cyber claims due to enhanced remote working, and cautioned all insurers to take precautionary measures to address such cyber risks and mitigate such risks when identified. Directive was also given to educate their staff on possible cyber risks and associated safeguards to be taken while working from home.

Do's

- Ensure that the Wi-Fi connection being used is password protected and cannot be breached easily
- Wifi password at home ought to be changed frequently
- Ensure that adequate software to protect the computer from external threats have been installed
- Timely assessment and training for employees to identify any breach in the system
- The insurer must be kept informed of the change in the working structure. As employees work out of office, this forms a part of material alteration risk that the insurer must be kept informed of
- Ensure that employees are informed, educated and aware of various traps hackers use
- Notify the authorised representative immediately of any breach and take corrective measures
- Create a crisis management and incident response team and formulate plans that may be executable by a remote workforce
- Ensure that no costs are being incurred without keeping the insurer informed or without consent

Don'ts

- Do not expose computers to potential viruses by downloading information from unauthorised / unsecured web pages
- Do not share the Wi-Fi connection with multiple persons, leading to breach of firewalls
- Do not share sensitive information with third parties unless an official sign off has been provided
- While handling customer data, ensure compliance of data protection policies

Conclusion

Given the current situation, we foresee work from home culture to continue for a longer period. While it will constantly evolve, organisations need to adapt with the times and come up with appropriate safety mechanisms. Working remotely doesn't have to be risky. However, without the right protocols and tested infrastructure in place, issues can escalate quickly and be harder to mitigate as compared to a centralised office environment. Companies should ensure that the organisation's cybersecurity practices are sufficient to comply with the prevailing data protection laws and other regulatory norms and to protect the business against sophisticated cyberattacks. Good practices ought to be implemented swiftly to tackle the ongoing issues surrounding the virtual world, particularly in light of the impending Indian data protection regime.

www.prudentbrokers.com

PRUDENT INSURANCE BROKERS PVT. LTD.

Registered Office 101, Tower B, Peninsula Business Park, G.K. Marg, Lower Parel, Mumbai - 400 013, Maharashtra, Tel: +91 22 3306 6000

CIN No.: U70100MH1982PTC027681 | License No. 291 (18th February 2020 to 17th February 2023)

Insurance is the subject matter of solicitation.

Advt2020May001