Secure Tomorrow

Minet

AON | Global Network Correspondent

MINET THOUGHT LEADERSHIP

Minet is a trusted pan-African advisor that meets the uncertainties of tomorrow by delivering risk and human capital solutions today. As the largest Aon Global Network Correspondent, Minet has access to a network of over 50,000 colleagues in 120 countries as well as to proprietary data, research and analytics which enable us to manage and secure the risks of tomorrow and provide clients with an unrivaled advantage. For more information, please visit www.minet.com

Risk. Reinsurance. People.

CYBER INSURANCE IN THE COVID-19 ENVIRONMENT

May 19th, 2020

With the unprecedented global pandemic of COVID-19, companies are adapting to the new reality of social distancing and self-isolation, practices encouraged by the government and health authorities, leading many businesses to transition large numbers of employees to remote working. Many of these employees, and for that matter employers too, have no prior experience in working remotely, and in most cases, are not even properly equipped to do so.

Remote working requires, among other things, equipping employees with the ability to connect to company servers from home. This necessitates providing the employees with the tools required to carry out their work efficiently, such as laptops, at home workstations, and remote access to secured networks and other company resources. As companies are grappling with challenges associated with the outbreak of Covid-19 and its attendant effects on large scale remote work, business growth & sustainability and on expense and liquidity management, organizations are increasingly relaxing their IT rules and policies. Such new IT policies include "bring and use your own device programmes" as organizations aim to increase employee mobility.

Unfortunately, the transition to work remotely will certainly come at an increased risk of cyber-attacks, an increased chance of data leakage, breach of data privacy regulations and other related cyber losses. Cyber risks faced by businesses today take different forms: in addition to hardware and/or software failure, the loss of portable devices such as laptops or smart phones, and the use of unsecured Wi-Fi connections by employees. Even more importantly, companies nowadays face sophisticated attacks from hackers targeting users seeking information on COVID-19. Given these risks, it is critically important for businesses to take steps to insure and protect themselves against such cyber losses.

CYBER INSURANCE-WHAT IS IT AND WHAT DOES IT COVER?

Cyber insurance provides protection and coverage for the security and privacy of digital information and losses resulting from data breaches. Cyber risk policies provide both first party and third-party coverage. Though each policy varies, a policy should be thoroughly reviewed prior to purchase.

First party coverages typically provided under a cyber insurance policy include:

- Expenses incurred by a company as a direct result of the breach, including remediation

/ extortion and notification expenses, regaining access, recovery, recreation as well as crisis management expenses; and
- Resultant costs such as business interruption and Public Relations.

Third party coverage under a cyber insurance policy typically provides coverage for liability in connection with losses suffered by customers as a result of the theft and use of their personal and/or financial data.

Most insurers/brokers also offer value-added services, such as network security testing, designed to help companies avoid and mitigate the effects of a data breach, and crisis management services. At Minet we furthermore offer risk transfer and have partnered with dedicated service providers enabling us to offer managed cyber security services, data-loss prevention, compliance and governance protocols, risk management, information security audit services, penetration testing, network security and content infiltration services.

Ensure That Your Cyber Insurance Policy is Comprehensive Enough to Suit Your Company's Needs

Coverages offered under cyber insurance policies vary considerably. When purchasing a cyber insurance policy, the policy wording, and more importantly the exclusions, should be closely reviewed with a professional to ensure the potential losses your company may face in the event of a data breach are covered. The type of coverage required will depend on the nature of the company, the types of information it stores within its secure network, as well as the types of activities the business participates in.

What Can Employees and Employers Do to Prevent Cyber Attacks?

Both employers and employees must take utmost care to protect themselves and confidential company information, especially while working remotely. Such steps include:

- Encouraging employees to pay attention to phishing emails, which are emails disguised with an enticing link, that when clicked on, can download malware onto a device and the company's systems;
- Ensuring employee devices are up to date on their anti-virus protection;
- Ensuring employees are working on secure, password-protected internet connections and avoiding the use of public Wi-Fi as much as possible;
- Reminding employees that personal email should not be used for any company business; and
- Urging employees to keep track of what they are printing at home and to shred confidential documents as soon as possible before they are disposed of.

Conclusion

The best way to protect your company from cyber risks is to ensure appropriate preventive measures are in place and that employees working from home, or with remote access to company data, are trained on how to implement these measures. We must all be diligent in protecting and securing sensitive business data and client information. However, when an attack does happen, it is crucial to have the right cyber risk insurance products in place to assist in dealing with the after-effects of a breach.

John Gangla | Assistant General Manager, MRS, Corporate Division | Minet Kenya