KYND

Why is cyber important?

Over the last decade, cyber security has become one of the top concerns in corporate culture. With each step businesses take to protect their valuable data and assets, cyber criminals are proactively looking to undermine their efforts by adopting more sophisticated techniques to diversify their attack vectors. In the digital age, when more and more businesses become hugely reliant on online services, it opens up even more lucrative opportunities for fraudsters.

Cybersecurity encompasses everything that pertains to protecting our sensitive data, personally identifiable information (PII), protected health information (PHI), intellectual property, and industry IT systems from theft and damage attempted by criminals and adversaries. Ransomware, Financial Fraud, and business interruption are the most serious risks facing any business connected to the Internet and the attack vectors can be thought of in two categories; 'human factors' including employee fallibility and social engineering, and 'operational factors' including email security, vulnerable software, misconfigured services & weak operational processes.

Gone are the days of simple firewalls and antivirus software being your sole security measures. To maintain the pace with an ever-evolving threat landscape, businesses need to be able to identify and address emerging threats before they become attacks.

Security incidents regularly affect businesses of all sizes across all sectors and often make the front page causing irreversible financial and reputational damage. When it comes to a data security breach or privacy loss, it isn't a matter of "if" but rather "when" it will happen. Cyber liability insurance is an essential aid in that response and is an exponentially growing market.

Gaps in Traditional Insurance

Many organisations may be operating under the belief that their existing insurance policies are enough to cover their data security and privacy exposures. Unfortunately, this is not the case and traditional insurance policies may be inadequate to respond to the exposures businesses face today. Consider these traditional policies:

General Liability

General Liability policies are typically triggered in response to Bodily Injury (BI) and Property Damage (PD) claims. A cyber event will not usually involve either BI or PD and General Liability policies typically don't offer cover for any first-party costs.

Crime

Crime policies typically respond to direct losses from employee theft of money, securities, or tangible property. Computer crime extensions usually exclude any third-party liability cover and may not sufficiently cover the loss of confidential information.

Property

Property policies typically respond to destruction or damage to tangible property resulting from a physical peril. The tangible loss then permits the business interruption and extra expense cover to respond. A cyber event, on its own, may not result in physical damage, yet the event can shut down a business resulting in substantial expense costs and loss of income.