If we talk about business in current times, it seems almost impossible without integration with the internet and E-commerce. Since more and more businesses are making use of the online world, the rate of cybercrimes is also rising. Although advanced cyber security systems, new software designs, and fresh laws are being introduced each year, there is still a higher probability of hacking incidents that lately make regular news in the headlines. Understanding the importance of cyber security is, therefore, the need of the day for all kinds of businesses, regardless of their operations being internet based or not.

**Are organizations prepared for a cyber security attack?**

In 2011, an Australian IT company named Distribute.IT that had 30,000 clients got hacked by a 25-years-old hacker, who deleted all the websites the company was hosting for its clients. Despite three weeks of continuous efforts, the company lost its standing in the IT market and eventually shut down.

Very few organizations actually understand their ability of "readiness" in response to a cyber-attack. Most of them usually lack human resource, proper incident response plan, technology, support systems, and security service suppliers. In order to be fully prepared for cyber-incidents, we need to develop a mindset of “what to do **when** it happens”, and not “what to do **if** it happens”. Hence it is important to be prepared with all the required technology and resources; to develop mechanism for gathering information in case of occurrence of an incident; to create interdependencies between processes; to build support systems; and to build contacts with suppliers who provide their expertise to help build a more “cyber-secure” environment.

**Who are the victims?**

The victims of cyber-attacks are not only large companies. In reality, small businesses are more frequently being successfully targeted by cyber criminals because of their lack of consciousness towards cyber security. Their attacks are becoming dangerously sophisticated and the resulting losses are even more devastating each passing day. Businesses that involve online purchases and deal in Payment Card Industry are even more prone to becoming a victim. Hence, every organization that has digitized information is at the brink of a digital parameter breach. There is now a greater chance of their valuable information assets being compromised.

**Are techies the only ones responsible for cyber security?**

Historically, cyber security of a company has been considered as the responsibility of the IT department only, which is a poor practice among organizations. In fact, all employees of a company should have a prepared mindset that a cyber-attack can occur any time, and strategies should already be in place for protection against them. Since it is usually the non-technical people of an organization that are soft targets for hackers, there is a dire need of creating information security awareness throughout the organizations. The IT department may only be responsible to clear out technical problems that arise as a result of a cyber incident, but it cannot avoid an incident from happening altogether if the other employees do not cooperate. Hence, the responsibility not only lies with the IT department but with all other departments of a business. When all departments, for example, legal affairs, corporate communications, regulatory department, audit and compliance, and business operations, along with senior management are aware of the significance of cyber security, it becomes easy to avoid potential threats and respond quickly to real threats that may arise.

In one of the incidents, the management of a major insurance company had to decide to shut down its network access immediately when the network security team confirmed a cyber breach; because they understood that security of their digital data loss was more valuable than the revenue loss that they had to face at that time. This saved the time required to brief the non-IT departments on such attacks, as they already had developed standard procedures. In return, it also improved in-time decision making during the cyber crisis, and averted the risk of high damage.

Organizations must conduct regularly information security awareness trainings and sessions to develop a cybersecurity approach in its culture. All personnel must regularly update, plan and practice secure cyber activities from e-commerce to even personal email usage.

**Frameworks for assessment of "State of Readiness" against a cyber attack**

There are various frameworks and standards to assess whether or not an organization has proactively planned for its cyber security concerns.

* **The ISO/IEC 27000 Series:** It provides basic guidance for the management systems of information security.
* **PCI DSS (Payment Card Industry Data Security Standard):** A set of requirements that help businesses securely process card payments and minimize card frauds by protecting client's information.
* **OECD Privacy Principles:** They help build appropriate controls into applications, information systems and networks. These are also the prerequisites of the privacy laws of most of the countries. OECD stands for Organization for Economic Co-operation and Development.
* **Australian Privacy Principles (APPs):** They outline how organizations falling under different categories need to use, handle and manage personal information.
* **COBIT5:** It is a comprehensive tool for checking information security and specific types of privacy controls being used for cyber security policies and standards.

**Board Members Need to Get Involved**

Board members hold the ultimate responsibility to instill the “cybersecurity awareness and readiness” approach in their organization. According to a promotional feature article by Australian Institute of Company Directors, board members and directors need to remember the following key points:

* One technical director does not have the sole responsibility for cyber security. All board members should get involved.
* It is important to be very conscious while using public Wi-Fi. A top executive can very well be a hacker's victim. Being extra conscious and vigilant is what their position as a leader in the organization requires them to be, so that others can follow.
* Self-check mechanism must be put in place, which will help consistently and constantly assess the board of directors for cyber security issues.
* New technologies must be explored, accepted and implemented. New ideas to help improve IT security must always be welcomed, e.g. cloud solutions.

Managing cyber risks is not any different than managing other business risks. Although the context is different but the fundamentals are same. Cyber security is a part of business. All board members need not understand every detail of it, but they do need basic awareness about its risks.

Even though IT professionals can technically cater cyber issues and provide their technical influences, only business owners can actually understand how even a temporary internet connectivity failure or loss of critical data can affect the bottom line.

**Let Us Help You be Prepared at all Times**

Our IT Security Consultancy services help you prepare for a cyber-secure environment.

We can help you in:

* Achieving your security goals and objectives by using our team of security, compliance and project management experts.
* Aligning with new Australian Privacy Principles to avoid privacy breaches, reputation destruction and financial consequences.
* Conducting ISO 27001 assessment and implementation.
* Finding security gaps, minimizing compliance obligations and making you achieve fast compliance.