Integration with the Internet and E-commerce has become an integral part of today’s business world, and as more and more businesses are getting online, the rate of cyber crimes are rising as well. Although, new and advanced cyber security systems, software and laws are being introduced each year, the threat of a hack incident is still likely, and one of the headline news lately. Therefore, understanding the importance of cyber security is the need of the day for all kinds of businesses whether their operations are internet based or non-cyber activities.

**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 fanatical efforts, the company lost its standing in the IT market and eventually shut down.

Very few institutes actually understand their ability of "readiness" in response to a cyber attack. Most organizations usually lack human resource, proper incident response plan, technology, information regarding an incident when it occurs, interdependencies between processes, support systems and external suppliers of cloud computing that provide secured cyber services.

**Who are the victims?**

Not only large, but even small businesses related to a variety of industries, are being successfully targeted by cyber criminals. Their attacks are becoming more frequent, 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.

**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 board members of a company should have a mindset that a cyber attack can occur any time and should have strategies already in place for protection against them. Because, it is the non-technical people of a board that are soft targets for hackers; either for financial ransom or hacking sensitive data of the organization and its clients that they may require for other reasons. That is why not only the IT department but all other departments of a business must also be aware and have adequate knowledge of potential cyber threats. When all departments, for example, legal affairs, corporate communications, regulatory department, audit and compliance, business operations, including senior management is aware of the significance of cyber security, it becomes easy to coordinate cross functionally upon potential cyber threats.

Once, the management of a major insurance company had to decide to shut down its network access immediately when the network security teams 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.

Therefore, the company executives should equally be involved in taking up cyber security as an integral issue, organization-wide.

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

There are various frameworks and standards for assessment of whether or not an organization has prudently planned for its cyber security concerns:

* One of the widely used frameworks is the ISO/IEC 27000 series, which provides basic guidance for the management systems of information security.
* Conformity to the PCI DSS (Payment Card Industry Data Security Standard), a collection of procedures and policies that help businesses to securely process card payments and minimize card frauds by protecting client's information.
* Information and cyber security practitioners ought to know the basics of OECD Privacy Principles so that they can build the appropriate controls into applications, information systems and networks. These are also the prerequisites of the privacy laws of most of the countries.
* The use of COBIT5, which is a comprehensive tool for checking information security and specific types of privacy controls being used for cyber security policies and standards.

As any of the board members who can access the internet through any means is likely a cyber crime target, therefore, they must regularly update, plan and practice secure cyber activities from e-commerce to even personal email usage. A consultant firm named Deloitte has also laid out a questions-based model that can help businesses identify their strengths and weaknesses regarding cyber security and implement it within their systems for safety and prosperity.

**Focus of executive managers and directors on cyber security**

* Holding the technical director solely responsible for cyber security should be avoided. Instead, all board members should get involved.
* The top executives should be very conscious while using public Wi-Fi and always assume that the company or even personally themselves will be hacker's victims. So, they should prepare for it by identifying loopholes within their business networks.
* Such checks and systems should be kept in place, which can help to consistently assess the board of directors for cyber security issues.
* They should not resist to indulge into information technology, and, accept and explore new technology ideas and how they can help to improve IT security, for example, cloud solutions.
* Executive heads should be aware that 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 merely a part of business, therefore, all board members need not to understand every detail of it but they do need basic guidance about its risks.

Even though IT professionals can technically cater cyber issues and provide its 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.