WHY IS CYBERSECURITY IMPORTANT FOR BUSINESS?

Cybersecurity has become a necessity for businesses of all sizes as their systems and networks containing sensitive and valuable data, have come under siege by malicious sources.

Without a cybersecurity strategy, your business cannot defend itself from cyber threats, leaving it vulnerable to threats, who will identify your business as an easy target. Along with the way technology has evolved over the years, there has been a steady increase in inherent and residual risks. Businesses have adopted more convenient methods of carrying out their operations. For example, data can now be stored on the cloud, i.e. many businesses use cloud services like Amazon Web Services, to store their valuable data. Although convenient, businesses rarely secure their information adequately while using these services, paired with an increase in attacker sophistication and this has led to a heightened level of risk that your business may succumb to a successful cyber-attack or data breach.

Businesses can no longer rely on simple solutions like their anti-virus or firewall to protect themselves from the impending risk of cyber criminals, who are becoming smarter and adept enough to evade these basic defenses. Businesses should work with a cybersecurity firm to help them build a cybersecurity strategy capable of providing a multilayered level of protection. It is also important to note that cybercrime should not only be taken seriously by businesses in heavily regulated industries, like healthcare or finance, but every business regardless of its size and type needs to prioritize the implementation of a cyber security program in their organization, as cybercriminals do not discriminate.

To help describe the importance of cybersecurity, below is an overview of the key components of cybercrime.

What is Cybersecurity?

Cybersecurity is, at its most simple, a series of processes and strategies put in place to protect a business's critical systems and sensitive information against cyber-attacks and data breaches, i.e. cyber threats. Cyber-attacks are increasingly more sophisticated as criminals are having an easier time evading traditional security controls, through the adoption of new methods of attack that implement artificial intelligence (AI) and social engineering. Businesses, as they adopt newer technology, need to also enhance their cybersecurity efforts to match it.

What Does a Cybersecurity Strategy Consist of?

A strong cybersecurity strategy consists of different layers of protection to defend your business against all kinds of cybercrime, including attacks that are designed to access, change or destroy data, extort money from your employees or business or aim to disrupt your day-to-day business operations.

Cyber strategies should consider the following:

- Infrastructure security

- Network security
- Application security
- Information security
- Cloud Security
- Employee security training and awareness
- Disaster recovery or business continuity

What is the Importance in Today's World?

As mentioned earlier, we are only becoming more reliant on technology and as a result, sensitive data like client and customer information is being stored online on cloud storage solutions like Dropbox or Google Drive. Businesses have become more dependent on computer systems, and this has only been boosted by the COVID-19 pandemic, with the majority of businesses having to adopt work from home solutions. This reliance along with the adoption of cloud services, smartphones and AI has led to various new security vulnerabilities that didn't exist only a few years ago.

Governments have also increased their regulation when it comes to cybercrime. For example, the General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU.

It forces organizations to:

- Communicate data breaches
- Appoint a data protection officer
- Require user consent to process information
- Anonymize data for privacy

With the GDPR, Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data to cloud services and breaches are a daily occurrence.

Similarly in Australia, the Office of the Australian Information Commissioner has introduced the Notifiable Data Breaches (NDB) scheme: any organization or agency the Privacy Act 1988 covers must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved. This has increased the reputational damage of a data breach for businesses in Australia.

Therefore, with the rise in regulation by government bodies on cybercrime, there has been an increase in importance and attention given to cybersecurity. Standard boards like the National Institute of Standards and Technology (NIST), have released a framework to help businesses understand their information security risks and improve their own cybersecurity measures in the hopes of defending against cyber-attacks and data breaches.

How Has Cybercrime Evolved Over the Years?

Criminals are more frequently targeting the information stored by businesses, with data theft being the most expensive and fastest-growing segment of cybercrime. This is supported by the increase in businesses storing identifiable information via cloud services, thus growing the exposure. However, it is important to note that theft is not the only possible goal, with some criminals choosing to either change or destroy information, with the hope of building distrust in an organization or government.

Social engineering continues to be the easiest form of cyber-attack with ransomware and phishing attacks being common methods of gaining entry into a business's critical systems or networks. Third-party risk is also increasing, as criminals choose to target third or fourth-party vendors, such as IT providers to gain access to businesses they partner with. All of the above trends have only heightened the need for and shown the importance of cybersecurity to be taken seriously by businesses.

What is the Impact of Cybercrime?

Cyber-attacks can impact every organization, regardless of size, in many ways including financial losses, dips in productivity, damage to reputation, legal liability and business continuity problems.

As reported by GlobeNewswire, cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015. According to The U.N. disarmament chief, cybercrime is up 600% as a result of the COVID-19 pandemic. All signs point to cyberattacks only increasing from here on out, therefore, businesses need to prioritize the implementation of a robust cyber security program or strategy.

How to Protect Your Business from Cybercrime?

There are a few simple steps your business can take to protect itself from cybercrime, below are some examples:

- **Educate employees -** Cybersecurity training is a strategy implemented by the IT and Security professionals in an organization to prevent and mitigate risk when it comes to compromising an organization's information security. These training programs are specifically designed to provide employees with clarity regarding their roles and responsibilities when it comes to upholding information security. A successful security awareness program helps employees understand proper cyber etiquette, the security risks associated with their actions and helps them identify cyberattacks they may encounter during their day-to-day operations.
- **Implement privileged access -** Privileged Access Management refers to the strategies and technologies organizations utilize to manage the privileged access and permissions for users, accounts, processes and systems across an IT environment. By strategically assigning employees the correct level of access (depending on their role and

responsibilities in the organization), the overall risk of suffering extensive damage from a cyber-attack is effectively mitigated, regardless of whether it's from an external actor or due to internal errors.

- **Monitoring, detection & response -** Businesses need to monitor their systems and networks on a 24/7 basis to ensure that there is no suspicious activity that may point to an attack or breach. If cybersecurity monitoring is not in place, it could lead to a delay in detecting that a threat is underway, and your business may not be able to respond in time to prevent it or reduce its impact.
- **Manage third-party risk -** Third-Party Risk refers to the potential threat presented to a business's employees and customer data, financial information and operations, from third-party vendors e.g., suppliers and other outside parties that provide products and/or services and have access to your systems. It's important for businesses to execute due diligence when partnering with a vendor e.g., ensuring that they have adequate information security policies in place and to continue to monitor that these standards are upheld when handling their valuable data.

These are just a few examples of initiatives businesses can adopt to increase their cybersecurity and reduce the chance of falling prey to a cyber-attack or data breach.