Need of Cyber Security

Cybersecurity is critical because it safeguards all types of data against theft and loss. Sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems all fall under this category.

Your company can't defend itself against data breach operations without a cybersecurity programme, making it an easy target for fraudsters.

Global connectivity and the use of cloud services like Amazon Web Services to store sensitive data and personal information are raising both inherent and residual risk. The chance of your firm being the victim of a successful cyber assault or data breach is on the rise, thanks to widespread inadequate cloud service configuration and increasingly adept cyber thieves.

Cybercriminals are becoming smarter, and their techniques are becoming more resilient to traditional cyber defences, so business leaders can no longer rely only on out-of-the-box cybersecurity solutions like antivirus software and firewalls.

Cyber risks can originate at any level of your company. Social engineering scams, phishing, ransomware attacks (think WannaCry), and other malware aimed to steal intellectual property or personal data must not be included in workplace cybersecurity awareness training.

Because of the increasing number of data breaches, cybersecurity is no longer limited to highly regulated industries such as healthcare. Even tiny organisations are vulnerable to irreversible reputational damage as a result of a data breach.

The importance of cybersecurity is increasing. Fundamentally, our society is more technologically reliant than it has ever been, and this tendency shows no signs of slowing. Data breaches that potentially lead to identity theft are now being shared openly on social media sites. Social security numbers, credit card numbers, and bank account information are now saved in cloud storage services such as Dropbox or Google Drive.

Whether you're a person, a small business, or a major corporation, you rely on computer systems on a daily basis. When you combine this with the advent of cloud services, bad cloud service security, cellphones, and the Internet of Things (IoT), you have a slew of new security risks that didn't exist only a few decades ago.

Even if the skillsets are getting more comparable, we must recognise the difference between cybersecurity and information security.

Cybercrime is receiving increased attention from governments around the world. The General Data Protection Regulation (GDPR) is a good example. It has raised the reputational harm caused by data breaches by requiring all EU-based businesses to:

- Notify people about data breaches.
- A data protection officer should be appointed.
- To process data, you must have the user's permission.
- To protect your privacy, anonymize your data.

The fashion toward public disclosure isn't always restrained to Europe. While there aren't anyt any countrywide legal guidelines overseeing statistics breach disclosure within side the United States, there are statistics breach legal guidelines in all states. Commonalities include: The requirement to inform the ones have an effect on as quickly as possible Let the authorities recognise as quickly as possible Pay a few type of fine

-Prof. Meera Kulkarni