APRIL 11, 2023 / EDUCATIONAL / INFORMATION TECHNOLOGY

Cybersecurity: A Necessity for Organisations

Do you want to protect your business from the devastating consequences of a cyberattack? The threat landscape has changed considerably in recent years, with the rise of mobile devices and social media platforms increasing the risk of attack.

Malicious actors leverage a variety of techniques such as phishing, malware, ransomware, zero-day exploits, targeted spear phishing campaigns and more in order to gain access to sensitive information or disrupt services.

Without proper security controls in place, organisations run the risk of costly data breaches that could lead to significant reputational damage and legal liabilities. Additionally, it is predicted that an astronomical **RM46.2 trillion** will be lost due to cybercrime by 2025.

Cybersecurity is no longer a nice-to-have; it's an essential part of protecting your organisation. Read on to find out the importance of taking the necessary steps to protect your organisation from cyberattacks.

The Importance of Cybersecurity

The Intensity & Complexity of Cyber Threats

Today's business operations are increasingly digital, with organisations relying on a variety of technologies to perform even basic functions. Unfortunately, with technology rapidly advancing, so is the sophistication of these attacks.

As the recent Verizon **Data Breach Investigations Report** of 20222 revealed, outsiders are the biggest threat, with hacking responsible for nearly half of all data breaches. Human motivation is the driving force behind 82% of the cases, malware in 13% of cases, and phishing or system intrusion pattern cropping up at 62%.

Cybercriminals use a range of sophisticated tactics and techniques to gain access to sensitive information or disrupt the normal functioning of networks. Advanced persistent threats (APTs) can remain undetected for extended periods of time while gathering intelligence about network infrastructure, user accounts, and system vulnerabilities.

Other forms of malware, such as ransomware, can cause massive disruption by encrypting data until payment is received. All types of attacks require significant effort to detect and remediate, making it crucial that organisations prioritise cybersecurity best practices.

It's a scary reality, but one that requires vigilance and action to stay safe.

The Hidden Threats of Crypto & Deep Web

Cryptocurrencies are digital currencies that exist outside of traditional banking systems and have become increasingly popular due to their ability to allow people to transfer money quickly and anonymously.

The anonymity associated with these virtual money transfers makes them difficult to track and trace, making it harder for organisations to protect from theft or fraudulent activities. Furthermore, hackers can use stolen credentials to access online exchanges and sell off virtual currency holdings or create fake accounts and purchase goods with stolen cryptos.

The "deep web" is another significant threat to businesses due to its ability to hide information from search engines. In other words, users must type in specific keywords in specialised software to find these sites.

The hidden content inside the deep web often contains malicious software and other illicit activities that could be used against a vulnerable organisation's system, making them a prime target for hackers.

Impact on Business Operations

Did you hear about the **71% of companies** globally hit by ransomware attacks in 2022?

The impact of cyber threats on an organisation can be far-reaching and extensive. In today's digital world, organisations rely heavily on their networks to conduct day-to-day operations and store valuable information.

A successful cyber attack could result in financial losses due to stolen funds or costly remediation efforts, the reputational damage that has long-lasting effects on the company's brand, legal action resulting from compliance violations, and more. The disruption of services caused by a cyber incident can also lead to operational downtime, which leads to lost revenue opportunities for business owners.

Cybercrime cost businesses an alarming **$4.35 million** in 2022 – and Malaysia felt the weight of it, with losses climbing to a staggering **RM600 million!** In short, the impact of a successful cyberattack can be devastating.

Clients' & Customers' Trust

Are you looking to build stronger relationships with your customers and improve your brand image? Then cybersecurity is crucial! Technology advancements have led to enhanced data collection capabilities as well as more sophisticated methods used by hackers to gain access to sensitive information.

Datto's 2022 State of Ransomware report showed that half of small to medium-sized businesses had antivirus and email/spam protection measures in place. This also includes network and cloud security protection. However, 34% of businesses have no cybersecurity protection in place but plan to put measures in place within the next year.

Organisations must be prepared to address these threats by implementing robust cyber security measures designed specifically for cryptocurrency and deep web usage cases. These may include multi-factor authentication protocols, encryption techniques and intrusion detection systems, among others.

Your customers need to trust that their data is secure when they shop with you.

Digital Data Safety

As more people use mobile devices to shop, bank, and communicate, the risk of losing sensitive information increases. People use computers for work, school, banking, shopping, entertainment, and everything else on a daily basis.

If someone hacks into a system, they can steal identities, damage confidential files, disrupt operations, cause physical harm, and even destroy lives. Cybersecurity measures help keep your data secure, preventing hackers from causing physical harm.

As technology continues to evolve, so does the way that businesses operate. Cybersecurity helps protect customer data and build trust with clients, prevents hackers from stealing identities, damaging confidential files, disrupting operations, and keeps your business running smoothly.

If you want to learn more about cybersecurity or any other aspect of the IT security audit, we can help! Drop us an email here at **enquiries@grayscale.my** to learn more.

APRIL 4, 2023 / EDUCATIONAL / INFORMATION TECHNOLOGY

IT Audit Explained

OCTOBER 5, 2022 / BUSINESS / EDUCATIONAL / MARKETING

Why is Cybersecurity important for an organization?

OCTOBER 13, 2022 / BUSINESS / EDUCATIONAL / MARKETING

How Can Cybercrimes Affect Your Business?

Leave a Reply

Your email address will not be published. Required fields are marked *

Your Comment *

Your Name *

Your Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

A subsidiary under TechnoDex Group of Companies.

Unit E-07-03, Menara Suezcap 2, KL Gateway, No. 2, Jalan Kerinchi, 59200 Kuala Lumpur, Federal Territory of Kuala Lumpur

T: +603 7932 0111

E: enquiries@grayscale.my