Citation

What are the biggest cyber security threats to your business?

A free checklist

v01

What are the biggest cyber security threats to your business?

The rate at which businesses are experiencing cyber security breaches is alarming. The latest UK government survey found that in the last 12 months, 39% of UK businesses identified a cyber attack. Within this, 31% of businesses estimate they were attacked at least once a week.[1]

Is your business at risk? Here's our guide to the top 7 cyber security threats you should be aware of.

1. Social Engineering

85% of breaches involve human interaction[2], hackers know that people are easier to trick than a system which means they are the biggest threat to your cyber security. Social engineering involves cybercriminals manipulating, influencing, or deceiving your employees into gaining control over their computer system or tricking them into handing over confidential data.

2. Phishing

Phishing ranks as the second most expensive cause of data breaches[3]. These attacks occur when cybercriminals impersonate a trusted contact or reputable source and entice a user to click a malicious link or open a malicious file. Phishing attacks can target your employees to steal login information or other details.

3. Ransomware

Ransomware attacks cost an average of $4.62 million[4]. Ransomware is a form of malware designed to block access to your computers or data. This data can then be corrupted, stolen, or deleted. Cybercriminals will then contact you to pay a ransom to unlock the data, although there is no guarantee this will happen even if a payment is made.

4. Weak Passwords

Have you ever used the same password for multiple accounts? It's likely your employees do too. Using passwords that can easily be guessed, or using the same passwords for multiple accounts, can quickly give a hacker access to your accounts and cause sensitive data to become compromised.

[1] Gov.uk – Cyber Security Breaches Survey 2022

[2] Verizon – Data Breach Investigations report

[3] IBM – Cost of a data breach report

[4] IBM – Cost of a data breach report

5. Malware (Malicious Software)

Hackers use malware to gain access to networks, steal data, or delete data from a computer. Malware often comes from malicious website downloads or spam emails. Once downloaded it infects your computer and the hacker is able to carry out their goal with a back door to access data, which can put customers and employees at risk. These attacks are also particularly damaging for small businesses as they can break devices, which require expensive repairs or replacements to fix.

6. Supply Chain Attacks

Supply chain attacks are rising and 66%[5] of these attacks focus on suppliers' code to target customer data. In supply chain attacks, hackers penetrate the supply chain security through third-party relationships. Suppliers, contractors, software providers - an attack on a single link can trigger a chain reaction that compromises the entire network.

7. Poor Cyber Hygiene

During the pandemic, the rate of cybercrime increased by 600%[6] and there is no slowing down. Attackers have taken advantage of the shift to new ways of working exposing gaps in online security. With remote and hybrid working here to stay, businesses need to be more vigilant than ever before. With more complex security issues and a lack of employee awareness and training on cyber security, poor cyber hygiene presents a big threat to your business.

[5]Enisa - European Union Agency for Cybersecurity

[6]ABC News (go.com) - The Latest: UN warns cybercrime on rise during pandemic -

Are you ready to respond?

With the continued growth in cybercrime, protecting against cyber attacks is one of the biggest challenges facing business owners. Without effective IT security, your business can't defend itself against data breaches and is an easy target for cybercriminals.

Any of these cyber security attacks could be detrimental to your business but there are things you can do to protect your business.

One popular approach is to implement an information security management system that is compliant with ISO 27001.

ISO 27001 is the leading international Standard for information security management. It's designed to help organisations of any size and in any industry protect their information security. It can give you the peace of mind you need by helping to keep valuable information assets safe and comply with the latest legislation.