Butterworth Spengler
Insurance Brokers

0151 494 4400
cyber@butterworthspengler.co.uk

Five Reasons Your Business Could Be A Cyber Attack Victim

CYBER

FEB. 2022

Cyber attacks can occur at any point in time, businesses fend off all types of cyber attacks around the clock, 24/7 365.

From insider threats, through social engineering, to phishing, malware cross site scripting cyber attacks can start anywhere at any time.

For the majority of businesses their normal working environment transformed overnight, with COVID-19 restrictions significantly increasing remote working and resulting in greater opportunities for cyber crime. No longer does a company have to just protect its business locations, there are now hundreds, even thousands of locations to protect. Even businesses created to support remote and flexible working struggled to manage the risk and exposure on such a large basis.

SMALL TO MEDIUM ENTERPRISE BUSINESSES

The majority of victims of cyber crime are Small to Medium Enterprises. Ransomware attacks, fund transfer fraud, phishing, vishing and social engineering are all made far easier with employees working remotely, combined with insecure home Wi-Fi.

1. LACK OF INVESTMENT

The media always report the big security breaches at major well known companies, however SME's are the more common victims of cyber crime and attacks. The reason you do not hear about SME's is that no business wants to have their reputation ruined by admitting they have been a victim of cyber crime. The Federation of Small Businesses estimates that SME's are facing up to 10,000 attacks daily. Cyber criminals see SME's as easy targets, even though the proceeds are less. A lot of SME's lack awareness and resources, investment in IT security and staff training on cyber security risks.

> **"The Federation of Small Businesses estimates that SME's are facing up to 10,000 attacks daily."**

2. SOCIAL ENGINEERING

Social engineering is a manipulation technique that exploits human error to gain private information, access or funds. In cyber crime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections or giving access to restricted systems. SME's are likely to be more exposed to social engineering because:

- They often have basic IT security in place
- They are unaware of the risks involved and often do not provide any training to employees who are the weakest link in IT security
- They work with a variety of third party partners to operate their business and these are the root cause of 41% of data breaches
- They almost always make and receive payments using bank transfer

3. PROMPT PAYMENT OF RANSOM

When faced with paying a ransomware demand to potentially get back online faster or enduring a long period of business crippling downtime, SME's will often feel their only option is to pay the ransomware demand. They are without the support of a dedicated cyber support specialist which a comprehensive cyber and data policy provides.

> **"Often when a ransom has been paid, the data is not returned or it is often found to be corrupted and unusable."**

Whilst committing a ransomware attack is a criminal activity, in general it is not a crime to pay a ransom demand, unless the payer knows or reasonably suspects that there are connections with terrorism or that this would breach sanctions regimes. Often when a ransom has been paid, the data is not returned or it is often found to be corrupted and unusable.

4. COLLATERAL DAMAGE

Developer Blackbaud was targeted by a cyber attack in May 2020, in which hackers broke into the developer's systems and stole personal data relating to donors and others who had shared those details with Blackbaud's customers. While the hack was detected and the hackers eventually locked out, they were able to copy personal data people had shared for various purposes with organisations that used Blackbaud's software.

SME's often find themselves as the collateral damage in large scale cyber attacks that have nothing to do with them, they often think that they are safe simply because they outsource their IT. When a cyber attack is launched against one of their technology providers, it is the businesses that rely on the technology provider that can be left facing business interruption losses, the associated costs of privacy notifications to clients, customers and are left with the reputation damage.

5. EXTERNAL IT USAGE

A significant number of SME businesses need to be connected electronically to multiple IT systems of partner companies, larger entities or businesses to assist them to operate and run their business. When cyber criminals are looking to hack into these larger entities which are generally more IT secure, they will look to target the larger entities downstream suppliers, as these SME's are often less IT secure and an easy route in. A large number of these IT relationships are visible through public available data.

0151 494 4400
cyber@butterworthspengler.co.uk
20-24 Faraday Road, Wavertree Technology Park, Liverpool, L13 1EH

Opening Hours
Monday - Friday
9am - 5pm

BIBA