STAY CYBER SAFE, A GUIDE.

Lycetts

Insurance Brokers
and Financial Services

CYBER-ATTACKS INCREASED 125%

CYBERCRIME STATS ARE SKY HIGH. DON'T BECOME ANOTHER STATISTIC.

Cyber security is becoming a dominant business priority. As technology continues to develop at an exponential rate, so too do the opportunities to expose businesses to a cyber-attack. The more we rely on technology to make our business run smoothly, the more vulnerable we become to over reliance on such systems should they fail in the event of an attack. The rise in remote working and cloud computing, along with more sophisticated and less easily detectable methods of attack, from phishing to malware, further compounds business' exposure to cyber risk.

MALWARE ATTACKS INCREASED

358%

BIG OR SMALL, YOU CAN BE A TARGET

A common misconception when it comes to cyber security is that some businesses are too small or 'under the radar' to suffer an attack.

1 BILLION
EMAILS EXPOSED

However, being a small operation has no bearing on vulnerability.

The very fact that smaller businesses are less likely to take cyber security seriously could make them an attractive target. In fact, 67% of SMEs feel that they do not have the in-house skills to deal with data breaches.

Although companies may see themselves as an 'offline' business, even riding schools and farms, forestry and rural estates use at least one digital tool in their day-to-day operations.

From using a computer to manage bookings or having a company website, to storing data in the cloud, or using employee email addresses, there are many seemingly 'innocuous' cyber risks that can leave businesses vulnerable.

Businesses should remember that an attack can not only be costly but can negatively impact on the business' reputation and has the potential to cause irreparable damage.

WHY CYBER SECURITY SHOULD BE A PRIORITY

This perceived lack of clarity on what businesses should be doing to become more cyber-secure is reflected in the low number of businesses investing in specific cyber security insurance.

Just one in ten (11%) businesses say that they have a specific cyber security insurance policy, and a further 15% of businesses say they have previously considered but ruled out having cyber insurance.

The two main reasons for not having cyber insurance include a lack of awareness of cyber insurance (23%) and considering themselves to have too low a risk to warrant it (22%).

OVERVIEW OF 5 COMMON FORMS OF CYBER-ATTACK

236.1 MILLION RANSOMWARE ATTACKS

1 MALICIOUS MALWARE

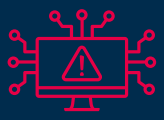
The user clicks a dangerous link which downloads software viruses. This can block access to the network's key components and steal confidential data without your knowledge.

2 PHISHING

An attacker impersonates a trusted contact and sends the victim fake emails. The victim opens the mail and clicks on the malicious link and attackers gain access to confidential information and account credentials.

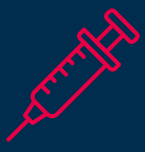
3 CYBER EXTORTION /RANSOMWEAR

Fraudsters threaten to expose or destroy data. Ransomware converts data into an unreadable format and only made accessible again by the payment of a ransom to the attacker.



4 DENIAL-OF SERVICE ATTACK

Attackers target systems, servers, or networks and floods them with traffic to exhaust their resources and bandwidth resulting in either shut down or slow down. This leaves legitimate service requests unattended.



5 SQL INJECTION ATTACK

Occurs on a database-driven website when the hacker manipulates a standard SQL query by injecting a malicious code into a vulnerable website search box. This results in the attacker being able to view, edit, and delete tables in the databases.

DON'T LET YOUR BUSINESS BE VULNERABLE

Your laptops, servers and computers can contain a lot of invaluable, business-critical data including personal information about your customers and suppliers, and also details of the online accounts that you access.

Equally, mobile technology is now an essential part of business, with more data being stored on tablets and smartphones than ever before.

As these devices often leave the safety of the office and home, they need even more protection than 'desktop' equipment.

That's why you should follow these helpful hints, from antivirus software to password protection, to protect your business from criminal cyber activity.

39% OF UK BUSINESSES HAVE EXPERIENCED A CYBER BREACH IN THE LAST 12 MONTHS

10 TOP TIPS TO PROTECT YOUR BUSINESS

1. Antivirus software should be used on all computers and laptops (often included free with most operating systems).

2. Only download apps for mobile phones and tablets from manufacturer-approved stores. These apps provide a certain level of protection from malware whereas third party apps from unknown vendors/sources may not have been checked.

3. Ensure that your IT software is always kept up-to-date with the latest versions or system updates from software developers. This update process is known as patching and is one of the most important things you can do to improve security.

4. Staff should only have enough access to IT systems to perform their role ('least privilege'), and businesses should only allow extra permissions to those who need it e.g. finance and HR administrators. This means if you are the victim of a phishing attack, the potential damage is reduced.

5. Most operating systems now include a firewall to protect your network - just remember to switch it on and update it when security patches are released!

6 Many phishing scams originate overseas and often low quality logos, poor spelling, grammar and punctuation are a sign of a scam. if in doubt - don't open it.

7 Emails addressed to 'valued customer' or 'friend' or 'colleague' can also be a sign of a phishing scam. Email filtering services attempt to send phishing emails to spam/junk folders. However, the rules determining this filtering need to be fine-tuned for your organisations needs.

8 Emails that contain a veiled threat often with a time-pressure attached that asks you to act urgently, such as 'send your details within 24 hours' or 'you have been a victim of crime, click here immediately', should never be opened.

9 All businesses, regardless of size, should take regular backups of their important data, make sure that these backups can be restored.

10 Avoid using obvious passwords, change all default passwords and always switch on password protection. You should also use two-step verification where possible (Multi-Factor Authentication).

TO ENSURE YOUR CYBER INSURANCE POLICY IS VALID, YOU MUST:

- Make sure regular backups are carried out
- change your passwords regularly
- Carry out regular software updates
- Regularly update firewalls and anti-virus/anti-malware protections
- Ensure you use Multi-Factor Authentication (MFA) - Lycetts use Google Authenticator, for example
- Train staff in payment procedures and teach them how to spot fraud (payment controls)

For a complimentary review of your insurance needs, highlighting any gaps or unnecessary cover, please contact us.

0191 232 1151
lycetts.co.uk
info@lycetts.co.uk

Lycetts | Insurance Brokers and Financial Services

Proudly part of the BENEFACT GROUP