CYBER GUIDE

Commercial Clients

towergate insurance

WHAT IS **CYBER** AND **CYBERCRIME?**

As technology develops, our reliance on it increases and in turn cyber related incidents are on the rise. Technology has allowed the world to stay connected more than ever before and it allows for convenience and access to information for millions of people. Unfortunately, this also means the same for criminals who can now access information and data like never before.

Cybercrime is criminal activity carried out using the internet and computer systems. It is undertaken by both individuals and criminal groups. Cyber criminals target networks and steal personal information in order to profit from it (usually for monetary gain). The increase in the way technology is used has altered the way that businesses operate. Money can be moved remotely as opposed to in person, and data can be stored electronically instead of using physical files. Most of a business's valuable assets are accessible to anyone, anywhere in the world. This changes the level of risk of them being lost, stolen or destroyed.

HOW **VULNERABLE** ARE YOU?

You are 9 times more likely to experience a cyber event than a property loss as a business*

If your business holds sensitive customer details, relies on IT and websites to conduct business or regularly processes payment card information, you should be thinking about how robust your data security measurements are, for example do you have all of your data backed up and stored on a different server?

25% of medium-sized businesses said that they have been asked directly by a current or potential customer about what cyber security measures they have in place**

Many small business owners believe that their business is too small to be targeted and therefore they don't invest in the necessary cyber security measures. Cybercrime is in fact on the rise each year and protecting your business against cybercrime is more important now than ever before.

If you think that you could benefit from having more protection around your business, it's a good idea to consider taking out Cyber & Data insurance, which covers losses relating to damage to or loss of information from, IT systems and networks.

*www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice
**Research conducted by YouGov on behalf of Zurich, July 2017

WHAT DO THE **THREATS** LOOK LIKE?

Cyber threats come in many forms, however the most common include:

PHISHING/'FAKE CEO FRAUD'

Cybercriminals using fake emails (phishing) and making calls (vishing) masking as someone they're not in order to gain access to information, data, and/or money. For example, an email pretending to be the owner of a business to approve an invoice for payment.

FUNDS TRANSFER FRAUD

Loss from unauthorised electronic funds transfers because of phishing, vishing or any other social engineering attack that results in the transfer of the funds to an unintended third party.

HACKING

Unauthorised access of a computer system. It works by identifying and exploiting weaknesses in computer systems and/or computer networks and gaining access to information. With telephone hacking, fraudsters crack the password to a phone network and programme the telephone system to repeatedly make calls to a premium rate number.

SMISHING

Text messages which appear to look like they have originated from reputable companies, individuals or the Government encouraging you to click on dangerous or harmful links.

VIRUSES, MALWARE AND RANSOMWARE

Often delivered or downloaded to computer systems with the intention of causing or threatening damage to software or data. Malware theft involves the opening of attachments from hackers that then automatically installs software which can allow access to your business's data and locks you out of your systems. There is often a request of a ransom to be paid, or the threat to reveal confidential information, unless a ransom is paid.

WEBCAM MANAGER

Criminals can take over your webcam and then blackmail you with the images.

KEYLOGGING

Hackers can record what you type on your keyboard. This usually gives away important passwords and in turn they may be able to access confidential information.

ADVERTS

Fake adverts may give criminals remote access to your computer through a specific link. Once they gain access to your computer, they can then access its contents.

There are implications that exposure to these risks can cause including income loss, damage management and repair, and the possibility of reputational damage if IT equipment or systems fail or are interrupted.

GDPR AND **YOUR RESPONSIBILITIES**

Another rising case of cybercrime is a data breach. With GDPR (General Data Protection Regulation) now in full force, client's personal data is something that every business should be safeguarding.

An example of this is when a Scottish hairdressing business was forced to pay a ransom to cyber criminals. Hackers locked the hairdressing company's data base and they threatened to erase all data. The company paid €1,000 in Bitcoins via a third party as they didn't want to risk losing any business. The company director revealed that since paying the ransom, the company have got a portion of their information back, however all bookings were lost as the appointment system was wiped.*

If you suffer a ransomware attack you may need help even if you pay the ransom. You may lose revenue while you cannot accept payments or bookings, and you may need help re-loading the data to ensure some isn't lost.

Cybercrime can impact any business no matter how large the company or organisation is. On 1st June 2020, a criminal gang attacked University of California San Francisco (UCSF). The university was instructed to log on by the criminals and the hackers demanded a ransom of $3 million. The UCSF representative explained that the coronavirus pandemic had been devastating financially for the university and said they could only pay $780,000, initially. The hackers demanded more and eventually the university paid 116.4 bitcoins ($1.14 million/£910,000) electronically. The issue the university now faces is that even though they paid the ransom to get their data back, they can't be entirely positive the hackers deleted the data, and they could potentially use it against them in the future for monetary gain.

Businesses need protection against financial loss if their customers' personal identifiable information (PII) is lost, stolen or leaked. From April 2018, GDPR means a company can be fined up to £20 million or 4% of its turnover (whichever is higher).

*Beazley (2019)

TIPS ON HOW TO **STAY SAFE ONLINE**

APP PERMISSIONS

Beware of who you share your location with. Deny permission requests from apps for information you feel like they don't need. Also choose applications from a reputable developer and only download from official app stores. If you are using a device for both personal and work reasons, then ensure your family and friends don't use it.

ANTIVIRUS SOFTWARE

Ensure your devices have an antivirus software installed on them. If they become infected, such software can help secure the devices and remove the virus.

LOCK SCREEN

If your device has a lock screen which needs your password to access information, your data etc. will be a lot more secure if your device is stolen than if you have no password protection in place.

SHARING INFORMATION

Be wary of what you are sharing online and who you are sharing it with. The more 'strangers' and people you don't know on social media who you accept friend requests from, the more at risk you are. The more information you share about yourself online gives hackers more information to use to impersonate you.

PASSWORDS

The more complex your password, the better. It is recommended that a password should be between 8 to 64 characters long. Using a passphrase which is memorable to you and nobody else is a good way to create a secure password. Visit **www.useapassphrase.com** to see how quickly a password can be cracked by hackers. Regularly change passwords across all devices and online platforms. Make sure you don't reuse your old passwords either.

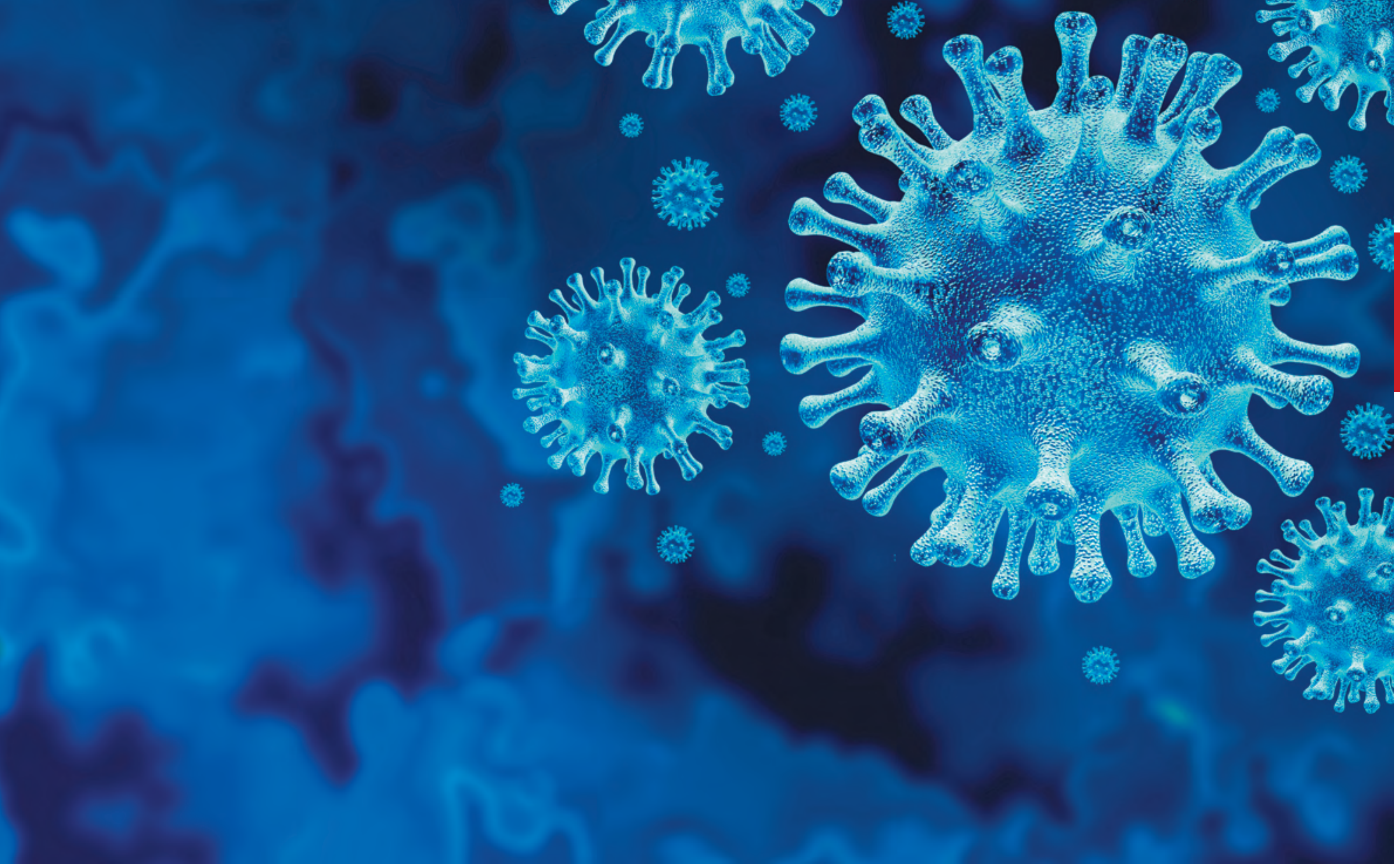
URGENT ACTION

If you receive an email or someone contacts you asking you to take urgent action right away, it may not be legitimate. Ask questions and check with people you trust to check the legitimacy of the request.

HOW TO **PROTECT YOURSELF** AGAINST CYBERCRIME

There are a number of things you can do to help protect yourself from cybercrime:

- Be extra vigilant with emails and texts. If something doesn't look right, no matter who it's from don't click on any of the content. Use an alternative way to contact that person or company to verify its legitimacy.
- Report suspicious Coronavirus related phishing scams to report@phishing.gov.uk (set up by GCHQ in April 2020).
- Ensure you follow your standard processes correctly especially when authorising payments and processing data.
- Regularly back up your data. This will make it easier to access data in the event of a breach.
- Invest in cyber protection insurance. This can help protect your business against the risks of a cyber-attack and can help limit the damage caused to your business and customers if you are affected by cybercrime.
- Individuals with access to highly sensitive data should be trained appropriately and considered for enhanced security protection. In addition, their digital footprints should be assessed and monitored to make it more difficult for them to be targeted, if compromised their confidential access to data could make for a more severe outcome.



CYBERCRIME AND **COVID-19**

The threat of cybercrime is one that we know already exists and is growing year on year. With the Coronavirus outbreak, however, cyber insurance is now more important than ever. We have seen how quickly this pandemic has brought the world to a standstill. A virtual virus can spread even quicker and can impact national and global networks that we are reliant upon.

A recent report by TSB Bank plc conducted in April found that 42% of people suspected they have been the target of phishing attacks during the COVID-19 outbreak. Scammers often imitate official bodies such as the Government, the NHS and even the World Health Organisation. They claim to be able to provide the recipient with details related to COVID-19 such as a list of infected people in their region. In order to access this information, the victim needs to click on the link which leads to a malicious website or is asked to pay ransom in Bitcoin.

The COVID-19 pandemic has already hit many businesses financially, slowing down operations and impacting productivity. The last thing a company needs upon returning to normal operations is to be impacted by a cyber incident. Cyber insurance can cover downtime costs, data breaches, and their consequences, as well as providing the technical, forensic and legal expertise needed to mitigate and remediate intrusions. Where cybercrime has occurred, Cyber insurance can cover such losses following fraud or social engineering, including extortion and the fraudulent transfer of funds.

RISKS TO CONSIDER WHEN THE **WORKFORCE RETURNS**

USE OF PERSONAL DEVICES

Working remotely has meant an increased reliance on personal devices for work use. If the device becomes compromised, it can potentially lead to malware being introduced into the business network where possible.

UNAPPROVED PERSONAL APPLICATIONS

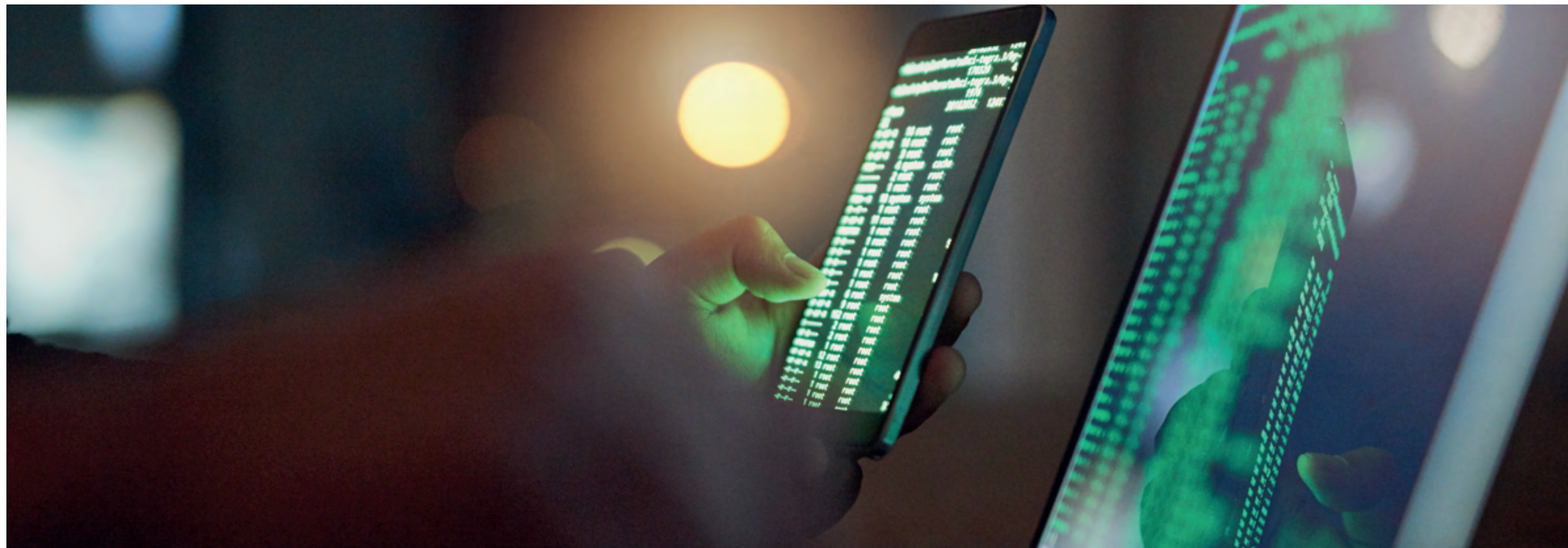
Such as teleconferencing software, and cloud storage applications etc. can increase exposure to phishing and malware attacks. These applications present similar risks to personal devices. Businesses should have a plan to identify and secure devices used while working remotely. This should involve identifying and fixing misconfigurations, patching, removing assets that shouldn't be online, malware scanning/cleaning, and if possible, restoring devices from a known backup.

REINTRODUCTION OF UNATTENDED SYSTEMS

Organisations may have ceased some or all IT functions during this period of remote work and pieces of IT infrastructure may have been taken offline for the duration. If this resulted in missed security patches, these systems may be newly vulnerable upon their reintroduction. Systems left online but unattended, may have been compromised by hackers waiting for a company's return to work before deploying malware in the business network. Critical systems that were unmonitored should be completely scanned with an antivirus tool to ensure no infections or intrusions have taken place.

HUMAN ERROR

Plays a leading role in the cyber vulnerability of an organisation. This can take the form of falling victim to phishing, unwittingly violating security practices, forgetting processes that have not been performed in months, accidental information leaking, etc. Upon return to work, there may be uncertainty about policy and practices regarding personal devices and applications in the workplace. Phishing attacks under the pretence of IT or financial services may be more persuasive and pressures of returning to standard operations may encourage complacency. Phishing education programs and training should be put in place.



CYBER INSURANCE TO **PROTECT YOUR BUSINESS**

CYBER EXTORTION INSURANCE

We can protect you if a hacker tries to hold your business to ransom with any final ransom paid (subject to policy limits), as well as the services of a leading risk consultancy firm to help manage the situation.

DATA RECOVERY SERVICES

In the event you lose any important data, we can provide data recovery services. This may incur an extra cost on your behalf – check your policy wording for more information.

CYBER BUSINESS INTERRUPTION

We can provide compensation for loss of income, including where caused by damage to your reputation, if a hacker targets your systems and prevents your business from earning revenue.

HACKER DAMAGE REIMBURSEMENT

We can reimburse you for the costs of repair, restoration or replacement if a hacker causes damage to your websites, programmes or electronic data.

To carry out a cyber assessment to identify the potential risks you may have, and for actions which can help resolve these risks, visit:

www.towergateinsurance.co.uk/liability-insurance/cyber-assessment

Or, if you want to speak to one of our specialist advisers about cyber protection, please call us on:

01438 739 739

or email us at:

caredivision@towergate.co.uk