Cyber, Data & Crime Risks

Is your business prepared?

thomascarroll
BROKERS LTD

Contents

46%

of UK businesses detected a breach in 2017

(Source: Government statistic)

60%

of small businesses fail within six months of a cyber-attack

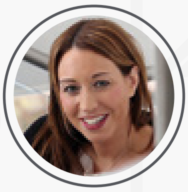
(Source: ICO)

Businesses are

40%

more likely to be victims of a cyber-attack than a burglary

(Source: Hiscox)



DATA & DIGITAL INSURANCE EXECUTIVE

Emma Buckley

Cyber, Data & Crime Risks

Are you prepared?

Cyber incidents, data breaches and cybercrime present increasing risks for businesses. Developing technology means new and emerging digital risks are frequent and challenging to manage.

Breaches can result in significant financial loss and reputational damage because data and customer relationship management systems are at the heart of most business operations.

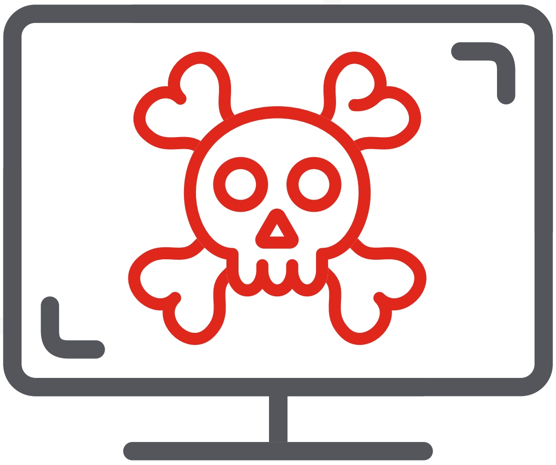
Cyber security is commonly mistaken as just an IT risk, but this is not the case. Breaches can be caused by accidental human error, which is considered a significant business risk. Breaches arising from human error can be as high as 95% (source: IBM statistics) and can be the result of simply losing a laptop or mobile phone containing personal or corporate data.

This briefing is designed to help you and your employees understand cyber security and prevent a breach. From training and IT security, to purchasing the right insurance to match your requirements, there are several positive actions you can take to help avoid business interruption, financial loss and reputational damage.

Are you protected?

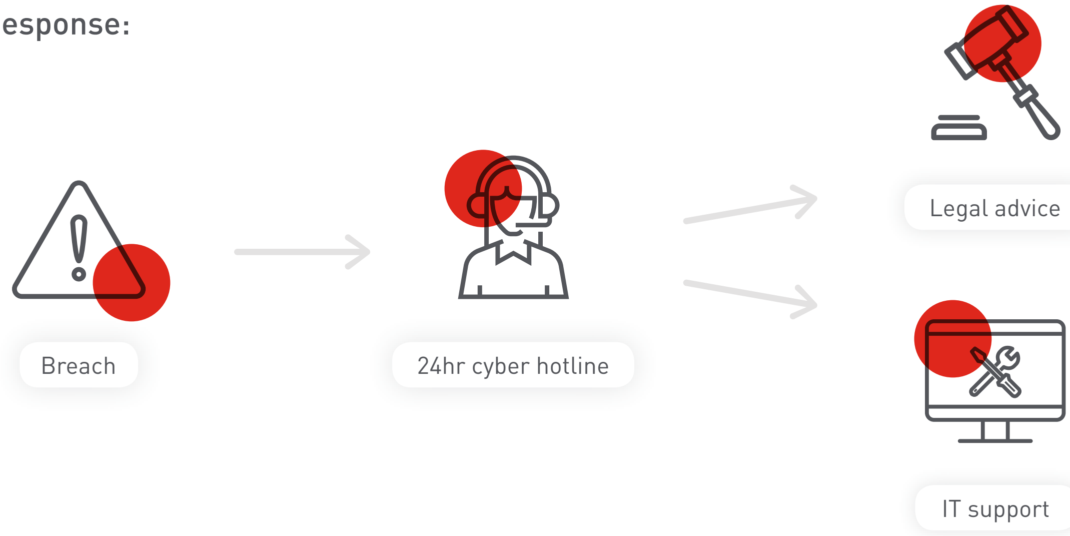
Insurance portfolios need to reflect the risk that businesses face right now, not the risks they faced 20 years ago. In a data-driven environment, it is important for business owners, directors and senior managers to prepare for any eventuality.

Reviewing your commercial insurance portfolio and introducing cyber insurance will help safeguard your business against modern risks. Thomas Carroll can advise you with a bespoke data and digital policy that will help guide and protect you and your business in the unfortunate event of a breach.



How cyber insurance can safeguard your business

First Response:



Breach → 24hr cyber hotline → Legal advice

→ IT support

Cyber Incident Response:

Legal

Legal advice on course of action

Respond to regulatory investigation and defend actions

IT security and forensic costs

Identify and remediate impact of a cyber breach

Contain malware and conduct forensic system investigation

PR

Coordinated communication to reduce brand damage

Client notification Credit & identity monitoring

Post notices to those affected by a cyber breach and manage inbound calls in relation to the notification

Provide credit and identity monitoring services

Cyber Liability and Data Protection:

Liability claims

Breach of confidential information including personally identifiable and payment card information

Investigations

Information Commissioner's Office (ICO)

Payment Card Industry (PCI)

Data Protection Act Breaches

Fines and penalties

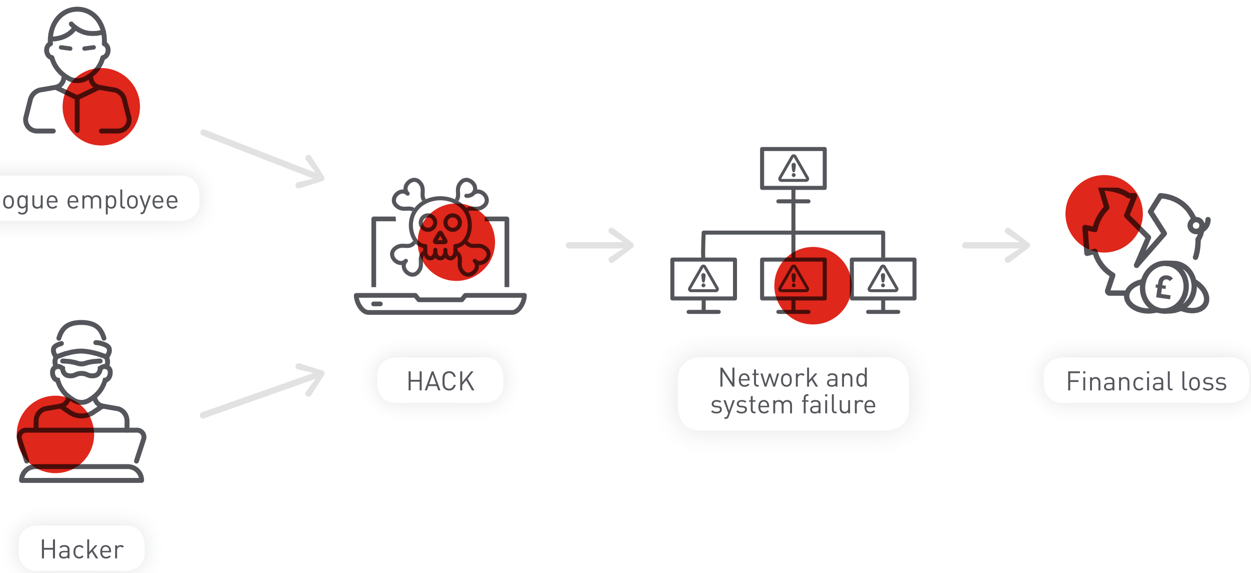
Where insurable by law, regulatory fines and penalties as a result of an investigation

PCI fines, penalties and assessments

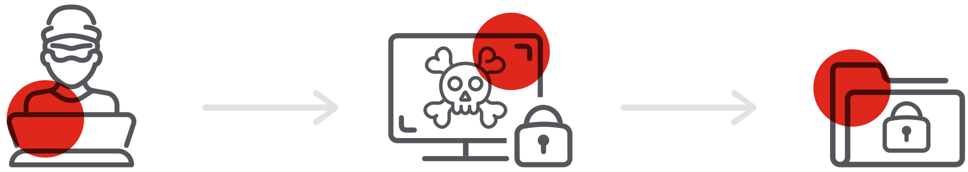
Network security liability

Transmission of malware to a third party or your system being used to carry out a denial of service attack

Network Interruption:



Cyber Extortion:



Hacker/ Extortionist

Ransomware in company network

Encrypted data

Ransomware is used to encrypt data until the company pays the hacker for a key to unlock their data

Insurance can be provided to cover losses from a ransom as well as fees paid to extortion specialists

Cybercrime:

Talk to Thomas Carroll about the optional extensions or additional policies available to cover cybercrime

Telephone hacking

Telephone systems hacked and calls made to premium rate numbers

Computer crime

Fund transfer fraud from a cyber security breach (hack)

Theft of funds

Theft of financial assets from bank or corporate credit cards by electronic means

Any phishing or social engineering attack resulting in your funds being transferred to a third party

Some insurers will also offer some loss-prevention tools that you can use to prevent a cyber incident or data breach. These can include vulnerability scans, IP blocking and employee awareness training portals. Speak to Thomas Carroll about the various tools available to you.

Act today to protect your business against cybercrime

There are several steps you can take to prevent a breach or hack:

1 Audit your technical controls through Cyber Essentials and Cyber Essentials Plus

2 Educate your employees

3 **Take anti-phishing measures**

4 **Consider penetration testing**

1. Cyber Essentials

Cyber Essentials is a government-backed scheme that has been developed to help protect businesses from the most common cyber-attacks. The scheme provides various package levels to suit different risk requirements.

The Cyber Essentials option gives businesses protection from common cyber-attacks and certification that can be used to demonstrate quality of care to clients. Cyber Essentials Plus is more enhanced and includes further specialist protection.

If you bid for central government contracts that involve handling personal or sensitive data, it is likely that a Cyber Essentials certification will be required.

For further information, please visit:
www.cyberessentials.ncsc.gov.uk/

2. Educate your employees

Human error is the main cause of cyber incidents and data breaches. It is important for employees to realise the implications of their actions when handling your data and IT systems.

Educating employees on how easily a breach can take place is the first step to protecting your business.

Help your workforce understand how a breach could be caused by:

- Losing a mobile phone
- Misplacing a memory stick
- Leaving a paper file on a train
- Emailing information to the wrong person or company
- Opening a phishing email
- Allowing someone access to your computer via a memory stick
- Allowing someone to use your Wi-Fi network or access your server

Thomas Carroll have put together some simple communication steps you can take to inform your employees and raise awareness of the potential dangers.

This guide will cover the following cyber risks:

- Device security
- Building security
- Portable media

Device security

Company devices can contain all manner of sensitive information such as copyrighted materials, patented technologies and personal data.

Keeping devices secure does not mean becoming paranoid, simply forming good habits. For example:

- When you leave your device, make sure it is protected with a lock screen
- Make sure your device is set to automatically lock after a few minutes of inactivity, in case you forget to lock it
- Never leave your device unattended in a public place
- Only allow others to use your device with your express approval and supervision

If you suspect someone might have used your device without your permission, or you suspect someone has done something that could put the system in jeopardy, contact your manager and/or IT service provider immediately.

Building security

Hackers gain access to a system by physically breaching a company's security measures. Typically, once someone has gained access to a building, he or she will be able to move around freely. It is important to follow these tips:

- Don't allow any unauthorised visitors into your workplace
- If someone claims to be there to see someone, confirm with that person that he or she is expecting a guest. Make sure that the co-worker comes out to greet the guest and escorts him or her around whilst the guest is on site
- Be sure to close and lock offices, filing cabinets, lockers or anything else that could contain sensitive information

Portable media

Sometimes you may find yourself transporting files on a memory stick, portable hard drive or other portable devices. When using portable devices:

- Password protect files
- Store important, sensitive and personal data on a separate device. This way if your device is stolen or lost, whoever finds it won't have access to your important information
- Back up your data so that if you lose a portable device, you're not losing your only copy of the data
- Do not leave devices unattended where they can be stolen or accessed
- Install updates, especially antivirus software and operating systems
- Avoid public Wi-Fi. Cyber criminals set up hot spots in public places like cafés, airports and hotels to try to get unsuspecting business travellers to connect. If you're going to use a Wi-Fi network, make sure you can trust its source. Make sure the network that you access is encrypted

3. Anti-phishing measures

What is social engineering?

Rather than attack a secure, encrypted system or database, cyber criminals use social engineering tactics to trick people into giving them access. That's why social engineering is often referred to as 'people hacking'.

How does social engineering work?

There are four basic psychological tactics that are almost always at play in social engineering scams:

- Fear of conflict. Social engineers exploit this by exuding confidence when they ask for information or physical access that they have no right to
- Getting a deal. Criminals are often known to use gifts and giveaways to get victims to let down their guard by downloading a file onto their computer
- Sympathy. By establishing rapport and building positive feelings, victims are too distracted to realise that they're being scammed
- Need for closure. Informed social engineers will have an answer to any challenge or question likely to come their way. It gives a sense that they have done their due diligence

Train your employees to avoid blind spots

Social engineering depends on psychological weaknesses and blind spots.

For example, criminals see email as the perfect tool for accessing networks, gaining valuable information and launching cyber-attacks. Employees can look out for malicious mail by:

1. Verifying the sender
2. Avoiding suspicious attachments
3. Avoiding links from unknown sources

What is phishing and spear phishing?

Phishing is a common and technologically simple scam that can put your co-workers and your company at risk.

Both phishing and spear phishing try to trick you into opening links that allow malicious programs onto your system or make you voluntarily give away the information that thieves want.

Phishing is a type of cyber-attack in which a hacker poses as a trusted source online in order to acquire sensitive information. More resourceful criminals are resorting to a modified and more sophisticated technique called 'spear phishing', in which they use personal information to pose as colleagues or trusted sources. These are much more difficult to identify as malicious.

How can you help your employees?

Advise your colleagues to:

- Never volunteer sensitive information. If an email asks for usernames and passwords, government-issued identification numbers or financial account information, STOP. These institutions would NEVER ask for sensitive information over an email
- Be suspicious of links asking for information. If you receive an email instructing you to enter information into a website by following a link, be careful
- Double-check the website address. Criminals have been known to purchase domains that look similar to legitimate websites, often differing by merely a letter. Make sure you're using the legitimate site before entering sensitive information
- Verify who you're communicating with. If you have any doubts about an email you receive, don't hesitate to verify the information. Look up the information of the person or company who contacted you and make a phone call

- Trust your suspicions. If the email asks you to do something that feels wrong or unusual, stop and think about it. Odd requests, careless typos or strange language can be subtle giveaways that it's not legitimate

Social media exposure

The popularity of social media has made it one of the top avenues of attack for cyber criminals. Here are just a few ways your social media accounts could put you at risk:

- Careless posts reveal sensitive information. Taking photos in the office may unintentionally reveal personal or proprietary information, which could allow competitors or cyber criminals unintended access to your company's intellectual property or systems
- Sharing information about your identity. A cybercriminal can use these clues about your life to access accounts or even steal your identity
- Infecting your computer with malware. As was the case with emails, criminals have begun to embed malicious code in links on social media posts. Once the malware is on your system, criminals can use it to access your system and steal sensitive information

Here's how you can help combat social media threats:

- Manage privacy settings to control who can see personal information
- Never click on suspicious links
- Think twice about posting anything, especially if it can cause harm or brand damage

4. Penetration testing

The only way to really know how secure your infrastructure and web applications are is to have them tested by qualified penetration testers. A penetration test involves you employing a company to simulate an attack on your systems which will highlight any vulnerabilities that could be exploited by hackers. This allows you to identify and rectify any vulnerabilities, so protecting your systems and providing your customers with confidence.

Crime Insurance v Other Policies

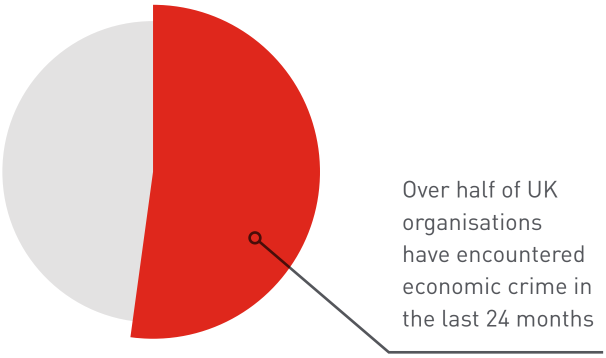
Organisations in any business sector can be victims of fraud, from inside or outside the company. Sometimes fraud is a one-off transaction but often it takes place over many years until it is discovered, having a massive financial impact on a business. Some crime examples include:

- Cybercrime
- Forgery
- Theft of property such as stock or cash
- Embezzlement

Impersonation Fraud

It is often wrongly believed that theft of money through fraudulent transfer is a cyber risk, when such losses fall under a Commercial Crime insurance policy. For example, a fraudster impersonating a colleague might email an employee of the organisation requesting several electronic transfers, and funds are moved to an overseas bank. This is surprisingly common, with many businesses not having the right insurance protection to cover losses.

Commercial Crime insurance is available to protect an organisation's money and property from theft, including deception. There may be an option to provide cover for some of these scenarios on a Cyber or Directors & Officers Liability policy extension, but not all policies provide the same breadth of cover.


Over half of UK organisations have encountered economic crime in the last 24 months

Cyber Insurance v Professional Indemnity Insurance

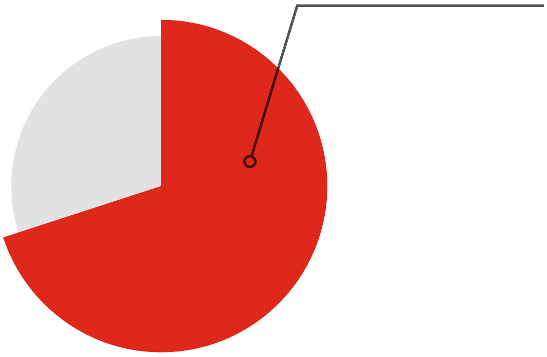
We have discussed why cyber protection is an important consideration for any business. However, some businesses will need a Cyber policy combined with a Professional Indemnity policy due to their trade.

Professional Indemnity is a form of liability policy that is designed to provide protection for businesses that give advice or professional services to their clients. This policy provides cover in the event that the service provided is inadequate, resulting in a client losing money.

When considering Professional Indemnity against Cyber cover, imagine a situation where confidential information or personally identifiable information is emailed to the wrong recipient, resulting in a civil case. Professional Indemnity cover will provide protection when these errors occur but will not provide many of the benefits of Cyber cover. These benefits include managing reputational risk, the cost of dealing with rectification and the initial costs of managing notification in the case of breaches of personal information.

Not all Professional Indemnity policies can provide cover for certain risks such as cyber risks, so it is important to look carefully at what is included in your policy.

Two-thirds of frauds are committed from outside an organisation



Cyber Insurance v Directors & Officers / Management Liability Insurance

If you are a director or officer, you could be deemed personally liable and subject to claims which can lead to high legal costs, fines, compensation and even imprisonment for actions carried out while performing your duties for the organisation.

Directors & Officers Liability insurance provides protection to the directors, partners and officers in a company to cover the costs of claims made against an individual. Without this cover, individuals in a business are unprotected if, for example, they have been negligent.

In the world of cyber risk, if a director acts negligently or inappropriately this could result in a data breach, costing the company a significant amount of money. If it is proved that negligence led to a data breach, a Directors & Officers policy can provide protection, including legal defence costs.

As well as having adequate Cyber insurance in place, organisations should look to insure their directors individually, in case a claim is brought against them personally following a cyber incident or data breach.

It is also important to ensure that there is no broad cyber exclusion and that the policy is affirmative that cover is provided. Increasingly, Directors & Officers policies include a data breach exclusion.

Getting the right protection

You can discuss all forms of insurance with Thomas Carroll: Cyber Liability, Crime Insurance, Directors & Officers and Professional Indemnity. We will ensure that any concerns you have are addressed.

Some Directors & Officers insurance policies can be extended to provide Crime cover (usually at low limits) and some Cyber policies provide Directors & Officers cover (but usually limited to cyber events).

Each policy provides you with different protection. Cyber insurance covers the incident response costs that would not be included on Professional Indemnity policies. Crossovers in cover can occur with regards to defending a claim for damages, for example. Understanding your risks and policy cover will ensure that you are not duplicating insurance costs or leaving important gaps in your protection.

Please contact Thomas Carroll so that we can discuss these covers with you fully.

Real Cyber and Crime insurance examples

The following examples have been published in the news and by insurance companies to highlight the modern risks faced by businesses across a range of sectors.

Accountants

Hackers sent a phishing email with bogus documents attached. Upon opening the attachment, a piece of key log in software was automatically installed which allowed the hackers to gather crucial access data and then log in to the firm's bank portal.

The insurers were contacted by the bank after several wire transactions to Nigeria. After managing to recall some of the wire transfers, the firm was left with a loss of £164,000 in electronic funds and costs of £15,000 in IT forensics.

Building contractor

A fraudulent yet almost identical email address for the managing director of a building contractor was created by fraudsters, who used it to instruct an individual in the accounts department to make a transfer of £50,000 to a new materials supplier.

The email stated that the new supplier was being used to source additional materials for a crucial job and urgent payment was required to secure the goods. The email was sent whilst the MD was on holiday. The fraudsters received the £50,000 before the transaction could be recalled.

Logistics

In 2017, a logistics company suffered malware, resulting in the business having to reinstall their infrastructure of 4,000 servers and 45,000 PCs. They suffered significant business interruption and still felt the effects a month later. The company was crippled for one week costing them an estimated $250m to $300m.

Healthcare

A care home looking after vulnerable children and adults suffered a breach. A laptop was taken which had a password stuck to it with a Post-It note. There is no proof that the data has been accessed, but due to the sensitive nature of the information the care home exceeded their cyber insurance limit of £100,000 and are expected to be under-insured by £50,000 to £75,000 for this breach alone.

Law firm

A financial controller in a law firm received a call from someone claiming to be from the firm's bank, explaining that some suspicious wire transfers had been flagged up on the business account. The caller said that the clients' remaining funds would be drained unless they froze the account. A password and pin were required to do so.

The financial controller provided this information as he didn't want to cause further loss. The loss that the law firm suffered as a result of social engineering was £89,900, which was wired to overseas accounts with no reimbursement from the bank, as the transaction had seemingly been authorised.

Luckily, this firm had purchased cyber insurance containing a cybercrime extension including social engineering and recovered all losses from their insurer.

How can Thomas Carroll help you?

Cyber incidents, cybercrime and data breaches are presenting challenging risks for businesses. With professional advice, there are several positive actions you can put in place to help avoid business interruption, financial and reputational loss.

Reviewing your commercial insurance portfolio and introducing cyber insurance (which is not covered as standard), is a good place to start. In the unfortunate event of a breach, your policy will guide and protect you and your business.

Chartered

Thomas Carroll holds Chartered status which is only achieved by companies who demonstrate commitment to maintaining the highest standards of technical competence and ethical conduct.

Independent

You can rest assured that Thomas Carroll's advice is objective and impartial, ensuring we always have your best interests at heart.

Award-winning

In 2018 Thomas Carroll was named UK Broker of the Year at both the British Insurance Awards and the UK Broker Awards.

TARIAN
ROCU | RCCU

Cyber Protect Officers from Tarian, Regional Organised Crime Unit together with South Wales, Gwent and Dyfed-Powys Police Forces, have a prominent role in raising awareness of cybercrime in our communities.

Please take a moment to read through this leaflet which highlights some easy ways to ensure you are better protected against the threat of cybercrime.

Cyber Protect Officers are dedicated to raising awareness of cybercrime, attending events and workplaces as well as contributing to online forums to educate staff about the importance of cyber security.

Cyber protect officers can update you on the latest cybercrime trends and provide helpful advice on how to protect your business. There is no charge for this service and officers will be happy to attend a venue of your choosing at a convenient time to you.

We work in conjunction with the National Cyber Security Centre (NCSC), National Crime Agency (NCA) and Action Fraud so the advice we share is consistent and reliable.

If you would like to contact the Tarian cyber protect team, please get in touch via the details below.

RCCU-Tarian@south-wales.pnn.police.uk **@TarianROCU** **www.TarianROCU.org.uk**

If you are unfortunate enough to become a victim of cybercrime, here are some tips to consider:

- Contact Action Fraud, the National reporting tool for cybercrime, on line or via telephone
- If demands are made through Ransomware:
- Do not pay - there is no guarantee that decryption details will be provided or that you will not be targeted again
- Delete all affected data and backup from a restore point to continue business operations as effectively as possible
- If data has been extracted, inform relevant customers and staff immediately
- Consider if you are obliged to report the breach to the UK Information Commissioner's Office
- Change relevant passwords as they may have been compromised during the attack
- Keep records of any email addresses, Bitcoin addresses or other identifiers included in demands
- If possible, preserve affected equipment for examination

TARIAN TOP TIPS

- Use a strong password to protect data. Keep your data backup separate from your computer and back up regularly
- Avoid Phishing attacks - Do not open anything from untrusted sources
- Report all instances of cybercrime
- Update operating systems and software
- Ensure all staff are aware and appropriately trained on the dangers of cybercrime and the importance of good cyber and personal security

Further useful resources are included below:

LITTLE BOOK OF CYBER SCAMS
www.tarianrocu.org.uk/the-teams

ActionFraud

ACTION FRAUD 0300 123 2040
www.actionfraud.police.uk

THE NCSC - SMALL BUSINESS GUIDE
www.ncsc.gov.uk/smallbusiness

Get Safe Online
www.getsafeonline.com

Act today to protect your business

Contact details:

0800 115566
hello@thomas-carroll.co.uk
www.thomascarroll.co.uk

Caerphilly | Swansea | Newport | Haverfordwest | Hereford | London

thomascarroll
BROKERS LTD

Sources: AIG & Tarian