CYBER & DATA

CRIME, FRAUD & FIDELITY GUARANTEE

towergate

THE RISKS

Cyber & Data

Digital technologies are an essential part of business today. All businesses rely on information technology (IT) infrastructure to some degree in order to increase their efficiency and improve their productivity. Which is precisely why cyber and data security breaches can be so damaging.

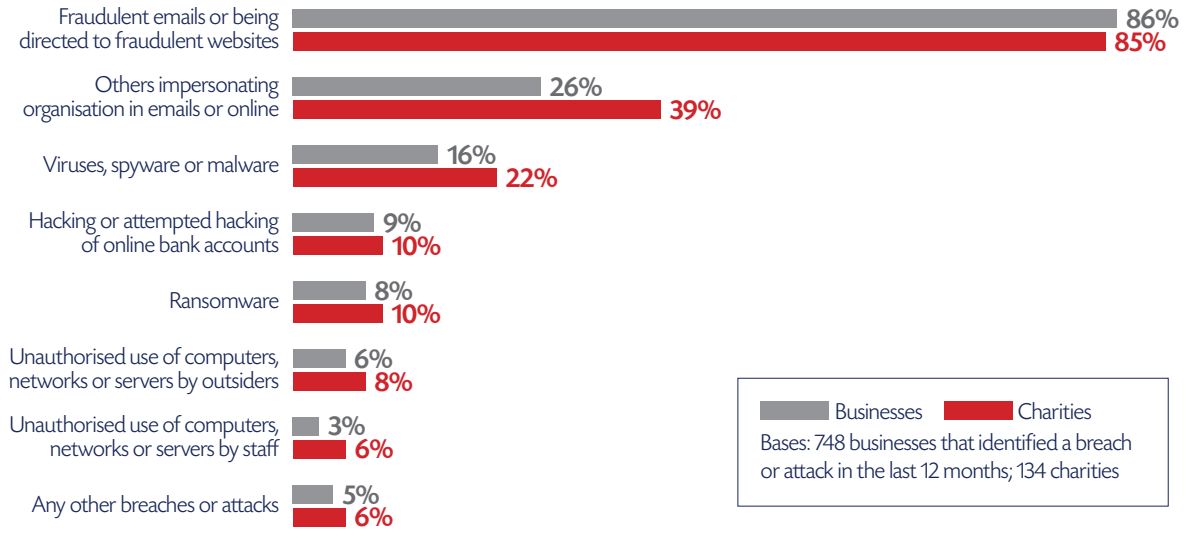
According to the Government's Cyber Security Breaches Survey 2020*, not only has the extent of cyber security threats not diminished; it has actually evolved and become more frequent. Almost half of businesses (46%) and a quarter of charities (26%) reported having cyber security breaches or attacks in the previous 12 months. It is higher among large businesses (75%) medium businesses (68%) and high-income charities (57%). Of the 46% of businesses who reported a cyber security breach, 32% experienced on at least once a week.

Among the 46% of businesses that identify breaches or attacks, one in five (19%) have experienced a material outcome, losing money or data. Two in five (39%) were negatively impacted, for example requiring new measures, having staff time diverted or causing wider business disruption. Similarly, among the 26% of charities reporting breaches or attacks, a quarter (25%) had material outcomes and over half (56%) were negatively impacted.

Where businesses faced breaches with material outcomes, the average (mean) cost of all the cyber security breaches these businesses have experienced in the past 12 months is estimated to be £3,230. For medium and large firms, this average cost is higher, at £5,220.

The most common type of cyber-attacks by far (experienced by 86% of businesses and 85% of charities who identified a breach or attack) are phishing attacks – staff receiving fraudulent emails or being directed to fraudulent websites.

Other types of breaches or attacks experienced are:



The implications that exposure to these risks can cause are wide-reaching. Some of the main issues are business interruption, income loss, damage management and repair, and the possibility of reputational damage if IT equipment or systems fail or are interrupted.

Why it's worth considering more specific, specialist insurance

Cyber is a very real, current threat to UK and Worldwide businesses. Existing insurance policies such as commercial combined, management liability or professional indemnity insurance may provide very limited elements of cover against cyber & data risks. But they are unlikely to be sufficient and businesses could find themselves exposed.

It is important that you understand if and what cover you have and how it would respond in the event on a cyber-attack or incident. Some policies will help you to respond to said attack, with 24/7 helplines to give immediate, practical assistance to mitigate costs; others will help to restore equipment and software after an attack.

Clients should particularly consider purchasing cyber & data insurance if they:

- Hold sensitive customer details such as names and addresses or banking information
- Rely heavily on IT systems and websites to conduct their business
- Process payment card information as a matter of course.

Crime/Fraud & Fidelity Guarantee

Economic crime continues to be a major concern for organisations of all sizes, across all regions and in virtually every sector. According to PwC's Global Economic Crime and Fraud Survey 2020**, 47% of the 5,000+ responders reported fraud in the previous 24 months, which is the second highest reported level of incidents in the past 20 years.

The top types of fraud reported were customer fraud, cybercrime, asset misappropriation and bribery and corruption. The losses reported due to fraud in the last 24 months totalled US$42 billion. These types of losses are complex – some costs can be tallied such as direct financial loss or costs due to fines, penalties, responses and remediation. But some costs are not easily quantified – including brand damage, loss of market position, employee morale and lost future opportunities.

Today, more than ever, it is obvious that businesses need to do everything in their power to limit their exposure to these risks and mitigate the cost of damages likely to be caused by electronic crime in the future.

* https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020
** https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) took effect on 25th May 2018 to replace the Data Protection Act 1998 and brought a step change in the responsibilities and duties around keeping data safely. GDPR was introduced to unify data laws around Europe.

The law now states the following:

- Data controllers and processors * are jointly liable for breaches of data protection.
- A mandatory requirement for all businesses to notify the Information Commission Office of any breach within 72 hours of becoming aware of the breach.
- A right for individuals to know when their information has been hacked.
- A mandatory requirement to notify all individuals who are affected by a breach of their personal data where this is deemed by the regulator to be a high-risk breach, i.e. that it could cause "significant harm"

Non-compliance of GDPR can result in fines of up to €20,000,000 or up to 4% of global turnover.

The implications are significant and reinforce the need for adequate Cyber & Data cover which includes cover for breach costs, including notification costs to affected individuals, which could be very high.

The requirements of Fair Presentation in the Insurance Act 2015 suggest that disclosure of a breach of data protection will be necessary when arranging your insurance in the future.

If you need advice on how insurance could apply to GDPR, contact your usual advisor.

*Controllers are all businesses holding data, whilst processors are all persons processing data including cloud and outsourcing companies processing data for their customers

CYBER & DATA INSURANCE – WHAT DOES IT COVER?

Cyber & Data insurance covers losses relating to damage to, or loss of information from, IT systems and networks. Policies generally include significant assistance with and management of the incident itself, which can be essential when faced with reputational damage or regulatory enforcement.

Cyber & Data risks fall into first party and third party liability.

First-party liability is the clients own assets which may include:

- Loss or damage to data or software programmes
- Business interruption from network downtime
- Cyber & Data extortion where third party threaten to damage or release data if money is not paid to them
- Customer and/or Third Party notification expenses when there is a legal or regulatory requirement to notify them of a security or privacy breach
- Repairs or replacement following system damage
- Regulatory actions & investigations and court attendance costs. Potentially cover for fines, where legally deemed insurable
- Crisis communication costs
- Reputational damage arising from a breach of data that results in loss of intellectual property or customers

Third-party liability covers the assets of others, typically your customers which may include:

- Security/privacy breaches, investigation and defence costs together with civil damages associated with them
- Multi-media liability, to cover investigation, defence costs and civil damages arising from defamation, breach of privacy or negligence in publication in electronic or print media
- Loss of third party data, including payment of compensation to customers for denial of access and failure of software or systems

CYBER & DATA – **CLAIMS EXAMPLES**

Ransomware

The managing partner at a private medical practice switched on his PC on a Monday morning to be greeted with a message stating that all patient records held on their network had been encrypted and **demanding a payment of £30,000** in bitcoin in exchange for the encryption key. He contacted an IT forensic specialist who confirmed the level of encryption, and confirmed that the only alternative to an encryption key would be wiping the ransomware from the network, risking the loss of all other critical data as part of the process. The last data backup was performed a week ago, meaning a significant amount of recent data was at risk, so they had no option but to pay the bitcoin ransom to protect their confidential data. They also engaged the forensic specialist to remove the remaining malware from their network at **a cost of £10,000.**

Denial of service attack

An international real estate client experienced a denial of service attack on their IT systems which was not only operationally damaging for the company, but also had the potential to severely impact upon its brand and market standing. The insurance policy not only covered the loss of income but also provided cover for PR expert support to mitigate any reputational damage.

Data ransom

An employee from a chain of opticians received an email to say that she had been caught speeding and clicked the button which offered to show a photograph of her being caught in the act. Shortly afterwards they received an email from someone in Russia to say that they had infected their systems with the Cryptolocker virus and that all files on its servers were encrypted. The encrypted files included patient records and software used to run the business. The Russians were asking for £400 in Bitcoins for the decryption key. The insurers approved payment of the ransom. Unfortunately this only recovered 90% of the files and they needed an IT contractor to help them recover the remainder. Their insurance policy covered this business interruption as well as the costs of being unable to trade for a couple of days and not being fully up-to-speed for a couple of weeks. **Total cost was £60,000.**

Data breach

An unencrypted memory stick was lost. It had been provided to a potential buyer as part of the due diligence process during a corporate acquisition transaction when it was stolen along with the owner's handbag from a public place. It contained personal and sensitive data of over 500 employees including home addresses and bank details. A fine was levied by the Information Commissioner's Office (ICO) and significant costs were incurred. In this scenario, the insurance policy allowed the firm to engage expert data risks or protection lawyers, liaise with the ICO and inform affected employees.

System hack

Hackers gained access to a Wholesalers email system and sent emails to all of their customers purportedly from either the Chairman or Finance Director saying that the Company has changed its bank details. Considerable time was spent contacting over 200 customers to tell them to ignore the email as it is not true. Several had already changed their records.

Virus

An Engineering Client had a virus planted into their system and were unable to use their IT for 5 days whilst their IT support resolved the problem. **Cost to rectify, £22,000** and all accounting, invoicing, stock control was affected, no payments could be made or received and it coincided with monthly payroll time which delayed paying the employees.

System breach

Client suffered an IT breach where 400,000 fake credit card statements were sent to their customers and other companies throughout the UK. The I.T. costs to rectify the damage plus estimated **loss of revenue cost £24,000**.

CRIME INSURANCE – **WHAT DOES IT COVER?**

Fidelity/Crime Insurance protects organisations from loss of money, securities, or inventory resulting from crime. Common Fidelity/Crime insurance claims include alleged employee dishonesty, embezzlement, forgery, robbery, safe burglary, computer fraud, wire transfer fraud, counterfeiting, and other criminal acts.

These schemes involve every possible angle, taking advantage of any potential weakness the company's financial controls. From fictitious employees, dummy accounts payable, non-existent suppliers to outright theft of money, securities and property. Fraud and embezzlement in the workplace is on the rise, occurring in even the best work environments.

Losses covered by crime insurance usually fall into two categories, although many polices combine both types of coverage:

- Money and security coverage pays for money and securities taken by burglary, robbery, theft, disappearance and destruction
- Employee dishonesty coverage pays for losses caused by most dishonest acts of your employees, such as embezzlement and theft – vulnerabilities can occur due to social engineering i.e. the cost of a fraudster influencing an employee to commit a crime.

Mandate Fraud

What is it?
An employee receives a letter or email, very often both, from what they believe to be a genuine supplier. The fake supplier will often identify that work is currently being undertaken, or has been completed recently but their bank details have changed and payment is to be made to a new account. After calls and emails to follow up on these instructions, an unsuspecting employee often facilitates the fraud by completing the payment. Sometime later, the genuine supplier will make contact and request payment, indicating that the original payment was not received. Further investigation will identify that the requests were fraudulent.

Loss example
A member of staff in the accounts department received an email purporting to be from contractors who were carrying out renovation works. It attached a letter confirming a change in bank details. The employee rang the number on the letter to confirm the change. Two further emails followed chasing payment of the amounts due. A payment of over £1,200,000 was authorised and wired. Three days later, the organisation that had authorised and wired the money received a call from the fraud department of their bank to raise suspicions over the transaction. It was quickly established that the money had been sent to an account that did not belong to the genuine supplier, and the money had gone into the account of the fraudster and had been quickly dissipated.

Fake CEO Fraud

What is it?
This common form of deception involves a fraudster impersonating a person of authority, such as a senior manager or IT representative. This 'fake CEO' strategy often leads to the targeted employee being persuaded to transfer funds to designated accounts, often overseas, in the belief they are assisting senior management to facilitate highly sensitive and important transactions.

Loss example – verbal
An employee was duped into believing that the CEO needed him to make confidential payments to a bank account in connection with an acquisition that was taking place. He was persuaded to circumvent established procedures because of the level of sensitivity that was involved in the deal. One transaction of over £500,000 was made, with six further transactions totalling more than £3,000,000 being stopped just in time. The employee was so convinced that the CEO had confided in him that he refused to reveal anything about the transactions until the real CEO attended a meeting with him. The CEO confirmed he knew nothing of the payments and that he had never spoken to the employee. It is thought that the fraudster listened to the CEO on a webcast and perfected his impersonation.

Social Engineering – Are your clients protected?
Fraudsters thrive in cyber & data space. Even if an organisation conducts seller background checks, employs fraud detection systems, segregates financial duties and educates employees on how to detect fraud, vulnerabilities may still exist. In our interconnected and technologically dependant world, refined and sophisticated techniques can penetrate even the best managed companies through social engineering fraud.

If you're worried about Social Engineering, please speak to us for more info.

CRIME – **CLAIMS EXAMPLES**

Funds Transfer Fraud

An employee received a call purporting to be from the company's bank saying there had been a problem with a payment, possibly caused by a virus. The caller told the employee that the payment would have to be made manually and managed to extract some, but not all, of the bank security code. The employee became suspicious and alerted managers who immediately informed the bank. The bank placed a stop on the account but not before eight transactions had been made, totalling **more than £430,000.**

Directly Dishonest

A company discovered that the Finance Director of a European subsidiary company had been manipulating its internal financial controls. Poor controls on segregation of duties and reconciliation of payments allowed the Finance Director to cover up the fact that he had regularly withdrawn small sums of money from the business and transferred them to his personal bank account. He also used a company debit card for personal expenditure. Over an eight year period **more than £700,000 was stolen.**

Project Mismanagement

On major projects the company initially placed a single order for parts. If further equipment was needed for maintenance purposes it was the project managers role to process these requirements. He ordered parts by forging a customer change request and customer signature. He would arrange for delivery of the parts to a private address from where he would sell the equipment on to his own customers . The employee future dated the invoices so they did not show as due or overdue. Only 250 of 45,000 orders were thought to be fraudulent, making the fraud difficult to detect. The fraud was perpetrated over five years and the loss paid was in **excess of £500,000.**

Vishing scam

The financial controller of a small high street solicitors firm received a call from someone purporting to be from their bank, advising that some suspicious electronic fund transfers had been flagged on their business account. The caller insisted that the firm may have already had funds stolen from their account and were in immediate danger of all of the remaining funds being drained unless an account freeze was implemented, apparently requiring the account password and unique security. Wanting to avoid any further loss, the financial controller gave the caller the requested security information, who then confirmed that the freeze had been successfully applied and that they would be in contact again once the situation was resolved. When the financial controller called the bank the next day for an update, they were told that no contact had been made with their firm, and that they would never ask for unique security details over the phone. They also confirmed that **a total of £89,991** had been transferred to three overseas accounts in nine separate transactions over the last 12 hours. Because these transactions had seemingly been authorised by the firm, using valid security information, they had been approved and were beyond recall, and furthermore no reimbursement or compensation was available to them.

Fake CEO Fraud – email

Criminals created a bogus email address for the Managing Director of a building contractor, virtually identical in format and appearance to the genuine one. They used this email account to instruct an individual in the firm's accounts department to make an electronic fund **transfer of £50,000** to a new supplier. The e-mail stated that the new supplier was being used to source urgent additional materials for a crucial job and that payment was required immediately to secure delivery of the goods. The e-mail was created while the MD was away on holiday so no face to face or verbal verification could be made. The payment was approved by the accounts manager and reached the criminal's account on the same day. As approval was given by an authorised individual at the firm, the bank were unable to recall the transfer, or offer any form of compensation.

Telephone hacking

A firm of insurance brokers installed a VOIP (web hosted) telephone system to manage their calls effectively and reduce their operating costs. A third party were able to use sophisticated software to access the VOIP network and programme the telephone system to make a high volume of automated calls to a premium rate number owned by the fraudsters. One month later, the firm was contacted by their telephone network provider as they had reached their account credit limit, having racked up **more than £25,000** worth of automated calls without their knowledge. Despite the telephone system provider acknowledging that the firm had been a victim of hacking, they insisted on the bill being settled in full.

CYBER –
RISK EXPOSURE SCORECARD

In recent years, cyber & data attacks have emerged as one of the most significant threats facing organisations of all sizes. The Internet and other network operations have created risks that were unheard of less than a decade ago. When cyber & data attacks (such as data breaches and hacks) occur, they can result in devastating damage, such as business disruptions, revenue loss, legal fees, and forensic analysis and customer or employee notifications.

It is important to remember that no organisation is immune to the impact of cyber & data crime. As a result, cyber & data liability insurance has become an essential component to any risk management programme.

INSTRUCTIONS: Begin by answering the questions below. Each response will be given a numerical value depending on the answer:
YES: 5 points **UNSURE:** 5 points **NO:** 0 points
After completing all of the questions, total you score to determine your organisation's level of cyber & data risk using the scale below.

EXPOSURE	YES	NO	UNSURE	SCORE
1. Does your organisation have a wireless network, or do employees or customers access your internal systems from remote locations?	☐	☐	☐	
2. Does anyone in your organisation take company-owned mobile devices (e.g. laptops, smartphones and USB drives) with them, either home or when travelling?	☐	☐	☐	
3. Does your organisation use Cloud-based software or storage?	☐	☐	☐	
4. Does your organisation have a "bring your own device" (BYOD) policy that allows employees to use personal devices for business use or on a company network?	☐	☐	☐	
5. Are any employees allowed access to administrative privileges on your network or computers?	☐	☐	☐	
6. Does your organisation have critical operational systems connected to a public network?	☐	☐	☐	
7. Does anyone in your organisation use computers to access bank accounts or initiate money transfers?	☐	☐	☐	
8. Does your organisation store sensitive information (e.g. financial reports, trade secrets, intellectual property and product designs) that could potentially compromise your organisation if stolen?	☐	☐	☐	
9. Does your organisation digitally store the personally identifiable information (PII) of employees or customers? This can include government-issued ID numbers and financial information.	☐	☐	☐	
10. Is your organisation part of a supply chain, or do you have supply chain partners?	☐	☐	☐	
11. Does your organisation conduct business in foreign countries, either physically or online?	☐	☐	☐	
12. Has your organisation ever failed to enforce policies around the acceptable use of computers, email, the Internet, etc.?	☐	☐	☐	
13. Can the general public access your organisation's building without the use of an ID card?	☐	☐	☐	
14. Is network security training for employees optional at your organisation?	☐	☐	☐	
15. Can employees use their computers or company-issued devices indefinitely without updating passwords?	☐	☐	☐	
16. Has your IT department ever failed to install antivirus software or perform regular vulnerability checks?	☐	☐	☐	
17. Can employees dispose of sensitive information in unsecured bins?	☐	☐	☐	
18. Would your organisation lose critical information in the event of a system failure or other network disaster?	☐	☐	☐	
19. Can employees easily see what co-workers are doing on their computers?	☐	☐	☐	
20. Has your organisation neglected to review its data security or cyber & data security policies and procedures within the last year?	☐	☐	☐	
TOTAL SCORE:				

ESCALATED RISK: 55-100	**MODERATE RISK:** 15-25	**HIGH RISK:** 30-50	**LOW RISK:** 0-10

Please send this to your usual advisor

CRIME V CYBER & DATA – **WHY DO COMPANIES NEED BOTH?**

Hopefully you are now a little clearer on both Crime and Cyber & Data Liability Insurance, so why should you have both?

It used to be so simple before the internet era... If your employee stole cash from your business or forged a cheque, a crime policy would cover it. If a non-employee broke into your business and stole money from the safe, a business combined would take care of the loss, under the peril of theft. But the world we once knew has changed, and continues to evolve both socially and technologically....and it's moving more quickly than ever.

Our businesses now depend upon technology and that reliance is expanding, as is cyber & data or 'data' theft and therefore our need to insure this evolving risk. What if that same employee stole your customer's credit card information or sold on sensitive information? What if your computer network were hacked and your customer's patented business information you were contractually obligated to protect was stolen? Would your crime policy still respond? The answer is, unlikely, hence why cyber & data liability insurance can be just as important as crime insurance to keep you and your reputation protected.

A crime insurance policy is designed to protect an insured business's assets from theft by both employees and other third parties. Defined as a first party coverage, the policy is triggered if the insured sustains a direct loss because of theft. It includes standard insuring agreements such as employee theft, forgery or alteration, theft on premises or in transit, counterfeit currency, computer fraud, funds transfer fraud and credit card fraud. It is very specifically designed to cover money, securities or other tangible property.

Cyber & Data liability policies are designed to insure loss of intangible property and the costs of rectifying systems damage. Think of your employee's HR records, your company's copyrighted material, formulas or documentation, your client's personal information etc. These are not tangible items, and thus not covered under a standard crime policy as mentioned above. The cyber & data liability policy also contains some first party coverages designed to directly reimburse you for specific costs and expenses associated with a breach.

Still unclear as to why do you need both? Each policy serves a purpose in protecting your business's assets, but neither covers all of the exposures. So in simple terms:

Crime cover is fraudulently taking money or property and Cyber & Data cover is IT system and data protection.

The truth remains that no 'standard' policy exists. And even though it may appear that crime exposures are addressed and covered in a cyber & data liability policy and vice versa, be wary of the exclusions, coverage triggers, and definitions. It is very likely that what may appear to be duplicate cover is far from it.

Here is a true life claims example demonstrating an incident where both a cyber and data policy and a commercial crime policy would respond.

Malware theft

Hackers sent a 'phishing' e-mail to an employee at small firm of accountants containing a bogus document attachment. By opening the attachment, the employee inadvertently installed a piece of key logging software on their PC, which allowed the hackers to gather and use secure access details to log into the firm's bank portal using genuine employee credentials. The firm was contacted by their bank after the hackers had initiated several wire transfers and batch payments from the insured's account to several accounts located in Nigeria. After checking with the employee whose credentials had been used to create the transactions, the firm instructed a specialist IT forensics company to establish what had happened and remove the offending malware from the system. Despite managing to recall some of the fraudulent wire transfers, the firm lost a **total of £164,000** from their accounts, and were left with a **£15,000 bill** for the forensics work – here is how one incident can involve both policies.

RISK MANAGEMENT – **ADVICE & PROTECTION**

Effective risk management will go a long way to protecting a business. Business leaders, or those tasked with the function of risk management, need to first understand their exposures before they can put in adequate controls. Risk management is a continuous process that at no point can be considered complete.

The National Cyber Security Centre (NCSC) have published 10 Steps to Cyber Security* which are:

1. Set up your risk management regime - Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

2. Network Security - Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

3. User education and awareness - Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

4. Malware prevention - Produce relevant policies and establish anti-malware defences across your organisation.

5. Removable media controls - Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

6. Secure configuration - Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

7. Managing user privileges - Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

8. Incident management - Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

9. Monitoring - Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

10. Home and mobile working - Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

*https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

CYBER & DATA – **COMMON TERMINOLOGY**

Access control
The process of granting or denying specific requests or attempts to:
- obtain and use information and related information
- processing services; and
- enter specific physical facilities.

Adware
Any software application that displays advertising banners while the program is running. Adware often includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge. And if you gather enough of it, adware slows down your computer significantly. Over time, performance can be so degraded that you may have trouble working productively. See also Spyware and Malware.

Advanced persistent threat
Advanced persistent threat (APT) usually refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attack. Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.

Asset
Something of value to a person, business or organization

Air gap
The physical separation or isolation of a system from other systems or networks.

Anti-Virus Software
Software designed to detect and potentially eliminate viruses before they have had a chance to wreak havoc within the system. Anti-virus software can also repair or quarantine files that have already been infected by virus activity. See also Virus and Electronic Infections.

App
Short for Application, typically refers to a software program for a smartphone or tablet.

Attachment
A file that has been added to an email–often an image or document. It could be something useful to you or something harmful to your computer. See also Virus.

Attack surface
All of an organisations internet-facing assets including both hardware and software. A larger number of such assets yields more potential vulnerabilities that an adversary can exploit to attack an organisation.

Authentication
The process of verifying the identity or other attributes of an entity. May also be used in multi-factor (or two factor) authentication, which refers to the process in which multiple methods are used to identify and authenticate an individual.

Authorization
The approval, permission or empowerment for someone or something to do something.

Backdoor (Trojan)
A piece of malicious software which allows someone to take control of a user's computer without their permission.

Backing up
To make a copy of data stored on a computer or server to lessen the potential impact of failure or loss.

Bandwidth
The capacity of a communication channel to pass data such as text, images, video or sound through the channel in a given amount of time. Usually expressed in bits per second.

Blacklist
A list of entities, IP addresses etc. that are blocked or denied privileges or access.

Blacklisting Software
A form of filtering that blocks only websites specified as harmful. Parents and employers sometimes use such software to prevent children and employees from visiting certain websites. You can add and remove sites from the "not permitted" list. This method of filtering allows for more full use of the Internet, but is less efficient at preventing access to any harmful material that is not on the list.

Brute force attack
A type of attack in which hackers use software to try a large number of possible password combinations to gain unauthorised access to a system or file.

CYBER & DATA – **COMMON TERMINOLOGY**

Blended Threat
A computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods–for example, using characteristics of both viruses and worms

Blog
Short for "Web log," a blog is usually defined as an online diary or journal. It is usually updated frequently and offered in a dated log format with the most recent entry at the top of the page. It often contains links to other websites along with commentary about those sites or specific subjects, such as politics, news, pop culture or computers.

Bring your own device (BYOD)
The authorised use of personally owned mobile devices such as smartphones or tablets in the workplace.

Broadband
High-speed data transmission system where the communications circuit is shared between multiple users.

Bug
An unexpected and relatively small defect, fault, flaw or imperfection in an information system, software code or device.

Business continuity management
Preparing for and maintaining continued business operations following disruption or crisis.

Clear Desk Policy
A policy that directs all personnel to clear their desks at the end of each working day, and file everything appropriately. Desks should be cleared of all documents and papers, including the contents of the "in" and "out" trays –not simply for cleanliness, but also to ensure that sensitive papers and documents are not exposed to unauthorized persons outside of working hours.

Clear Screen Policy
A policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially. Typically, the easiest means of compliance is to use a screen saver that engages either on request or after a specified short period of time.

Certification
Declaration that specified requirements have been met

Certification body
An independent organization that provides certification services.

Chargeback
A payment card transaction where the supplier initially receives payment but the transaction is later rejected by the cardholder or the card issuing company. The supplier's account is then debited with the disputed amount.

Cloud
Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services. Resources can include infrastructure, platform or software services.

Cloud computing
Delivery of storage or computing services from remote servers online (ie via the internet).

Command-and-control server
A computer that issues instructions to members of a botnet.

Common text
A structure and series of requirements defined by the International Organization for Standardization, that are being incorporated in all management system International Standards as they are revised.

Cookie
A small file that is downloaded by some websites to store a packet of information on your browser. Companies and organizations use cookies to remember your login or registration identification, site preferences, pages viewed and online "shopping-cart" so that the next time you visit a site, your stored information can automatically be pulled up for you. A cookie is obviously convenient but also presents potential security issues. You can configure your browser to alert you whenever a cookie is being sent. You can refuse to accept all cookies or erase all cookies saved on your browser.

Credentials
A user's authentication information used to verify identity - typically one, or more, of password, token, certificate

Cyber
Relating to, or characteristic of, the culture of computers, information technology and virtual reality (OED)

Cyberbullying
Sending or posting harmful, cruel, rude or threatening messages, or slanderous information, text or images using the Internet or other digital communication devices.

CYBER & DATA – **COMMON TERMINOLOGY**

Cyber essentials
A government-backed cyber security certification scheme that sets out a good baseline of cyber security. The base level requires completion of a self-assessment questionnaire, which is reviewed by an external certifying body. Cyber essentials plus adds an extra level by requiring tests of systems to be made by the external body.

Darknet
A darknet is a private, distributed P2P file sharing network where connections are made only between trusted peers – sometimes called "friends" (F2F) – using non-standard protocols and ports. Darknets are distinct from other distributed P2P networks as sharing is anonymous (that is, IP addresses are not publicly shared), and therefore users can communicate with little fear of governmental or corporate interference.

Data loss prevention (DLP)
A set of procedures and software tools to stop sensitive data from leaving a network.

Data server
A computer or program that provides other computers with access to shared files over a network.

Data at rest
Describes data in persistent storage such as hard disks, removable media or backups.

Declaration of conformity
Confirmation issued by the supplier of a product that specified requirements have been met.

Denial of Service Attack
The prevention of authorized access to a system resource or the delaying of system operations and functions. Often this involves a cyber criminal generating a large volume of data requests

Digital Certificate
The electronic equivalent of an ID card that establishes your credentials when doing business or other transactions on the Web. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Digital footprint
A 'footprint' of digital information that a user's online activity leaves behind.

Domain name system (DNS)
The phone book of the internet. It allows computers to translate website names, like www.hiscox.com, into IP addresses so that they can communicate with each other.

DNS hijacking
An attack which changes a computer's settings to either ignore DNS or use a DNS server that is controlled by malicious hackers. The attackers can then redirect communication to fraudulent sites.

DMZ
Segment of a network where servers accessed by less trusted users are isolated. The name is derived from the term "demilitarised zone".

Drive-by download
The infection of a computer with malware when a user visits a malicious website, without the user specifically initiating the download.

Download attack
The unintentional installation of malicious software or virus onto a device without the users knowledge or consent. May also be known as a drive-by download.

Dumpster Diving
Recovering files, letters, memos, photographs, IDs, passwords, checks, account statements, credit card offers and more from garbage cans and recycling bins. This information can then be used to commit identity theft.

Electronic Infections
Often called "viruses," these malicious programs and codes harm your computer and compromise your privacy. In addition to the traditional viruses, other common types include worms and Trojan horses. They sometimes work in tandem to do maximum damage

Encryption
The process of converting information or data into a code, so that it is un-readable by anyone or any machine that doesn't know the code.

Endpoint
An internet-capable hardware device. The term can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers, etc.

End user device (EUD)
Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.

CYBER & DATA – **COMMON TERMINOLOGY**

End User License Agreement (EULA)
A contract between you and your software's vendor or developer. Many times, the EULA is presented as a dialog box that appears the first time you open the software and forces you to check "I accept" before you can proceed. Before accepting, though, read through it and make sure you understand and are comfortable with the terms of the agreement. If the software's EULA is hard to understand or you can't find it, beware!

Evil Twins
A fake wireless Internet hot spot that looks like a legitimate service. When victims connect to the wireless network, a hacker can launch a spying attack on their transactions on the Internet, or just ask for credit card information in the standard pay-for-access deal. See also Man-in-the-Middle Attacks.

Exploit
An attack which takes advantage of a vulnerability (typically a flaw in software code) in order to access or infect a computer.

File-Sharing Programs
Sometimes called peer-to-peer (P2P) programs, these allow many different users to access the same file at the same time. These programs are often used to illegally upload and download music and other software. Examples include Napster, Grokster, Kazaa, iMesh, Ares and Limewire.

Firewall
A barrier between networks or parts of a network, blocking malicious traffic or preventing hacking attempts. The firewall inspects all traffic, both inbound and outbound, to see if it meets certain criteria. If it does, it is allowed; if not, the firewall blocks it.

Flooding
An attack that attempts to cause a failure in the security of a computer by providing more input, such as a large volume of data requests, than it can properly process

Gap analysis
The comparison of actual performance against expected or required performance.

Grooming
Using the Internet to manipulate and gain trust of a minor as a first step towards the future sexual abuse, production or exposure of that minor. Sometimes involves developing the child's sexual awareness and may take days, weeks, months or in some cases years to manipulate the minor.

Hacker
Someone who violates computer security for malicious reasons, kudos or personal gain.

Hacktivism
Used to describe hacking activity carried out for a political, ethical or societal ends.

Hard disk
The permanent storage medium within a computer used to store programs and data.

Hashing
A process that uses an irreversible encryption algorithm to turn a data entry into a random alphanumeric value. Typically used to protect passwords from compromise in the event that a malicious actor gains access to the database where they are kept. Often combined with 'salting' (see below).

Honeypot (honeynet)
Decoy system or network to attract potential attackers that helps limit access to actual systems by detecting and deflecting or learning from an attack. Multiple honeypots form a honeynet.

HTTPS
When used in the first part of a URL (e.g., http://), this term specifies the use of hypertext transfer protocol (HTTP) enhanced by a security mechanism such as Secure Socket Layer (SSL). Always look for the HTTPS on the checkout or order form page when shopping online or when logging into a site and providing your username and password.

Hybrid Attack
Builds on other password-cracking attacks by adding numerals and symbols to dictionary words. See also Dictionary Attack and Brute Force Attack.

Identification
The process of recognising a particular user of a computer or online service.

Incident
An incident is an event attributable to a human root cause. This distinction is particularly important when the event is the product of malicious intent to do harm. An important note: all incidents are events but many events are not incidents. A system or application failure due to age or defect may be an emergency event but a random flaw or failure is not an incident.

CYBER & DATA – **COMMON TERMINOLOGY**

Incident investigation
The investigation seeks to determine the circumstances of the incident. Every incident will warrant or require an investigation. However, investigation resources like forensic tools, dirty networks, quarantine networks and consultation with law enforcement may be useful for the effective and rapid resolution of an emergency incident.

Incident response team
The incident coordinator manages the response process and is responsible for assembling the team. The coordinator will ensure the team includes all the individuals necessary to properly assess the incident and make decisions regarding the proper course of action. The incident team meets regularly to review status reports and to authorize specific remedies. The team should utilize a pre-allocated physical and virtual meeting place.

Incident response plan (IRP)
A set of predetermined and documented procedures to detect and respond to a cyber incident.

Infrastructure-as-a-service (IaaS)
Provision of computing infrastructure (such as server or storage capacity) as a remotely provided service accessed online (ie via the internet).

Inspection certificate
A declaration issued by an interested party that specified requirements have been met.

Instant messaging
Chat conversations between two or more people via typing on computers or portable devices.

Internet service provider (ISP)
Company that provides access to the internet and related services.

Intrusion detection system (IDS)
A device or software application that monitors a network or systems for malicious activity or policy violations, with any unusual activity being flagged.

Intrusion prevention system (IPS)
A proactive version of IDS that can automatically take actions to block suspicious behaviour.

Insider threat
A person or group of persons within a company who pose a potential risk through violating security policies, either maliciously or negligently.

'Just in time' manufacturing
Manufacturing to meet an immediate requirement, not in surplus or in advance of need.

Keylogger
A type of malware that can secretly record a user's keystrokes and send them to an unauthorised third party.

Leased circuit
Communications link between two locations used exclusively by one organization. In modern communications, dedicated bandwidth on a shared link reserved for that user.

Local area network (LAN)
Communications network linking multiple computers within a defined location such as an office building.

Management system
A set of processes used by an organisation to meet policies and objectives for that organisation.

NIST cybersecurity framework
A set of standards, best practices, and recommendations for improving cyber security. It is industry, geography and standards agnostic, and is outcome rather than input-focused.

Network access control (NAC)
A method to bolster security by restricting network access to those devices that comply with a defined security policy.

Network firewall
Device that controls traffic to and from a network

Outsourcing
Obtaining services by using someone else's resources.

Operating System (OS)
Programs that manage all the basic functions and programs on a computer, such as allocating system resources, providing access and security controls, maintaining file systems and managing communications between end users and hardware devices. Examples include Microsoft's Windows, Apple's Macintosh and Red Hat's Linux.

Passing off
Making false representation that goods or services are those of another business.

Password
A secret series of characters used to authenticate a person's identity.

CYBER & DATA – **COMMON TERMINOLOGY**

Password Cracking
Password cracking is the process of attempting to guess passwords, given the password file information. See also Brute Force Attacks, Dictionary Attacks and Hybrid Attacks.

Password Sniffing
Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Personal firewall
Software running on a PC that controls network traffic to and from that computer.

Personal information
Personal data relating to an identifiable living individual.

Patches
Software and firmware add-ons designed to fix bugs and security vulnerabilities.

Payment card industry data security standard (PCI-DSS)
An information security standard created by PCI-SSC (see below) that governs how companies accepting payments by credit/debit card have to handle and protect that information. There are four tiers of governance, based on the volumes of transactions that a company is handling, from level 4 at the bottom end to level 1 at the top. The exact boundaries of these tiers are set by the individual card brands.

Payment card industry security standards council (PCI-SSC)
The body responsible for developing and promoting the PCI-DSS and relevant tools to aid compliance. Founded by the five main card bards (Visa, Mastercard, American Express, JCB and Diners) and supported by an 'advisory board' made up of representatives from major partners (retails, processors, banks, etc.).

Platform-as-a-service (PaaS)
The provision of remote infrastructure allowing the development and deployment of new software applications over the internet.

Penetration testing
A process whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Pentest
Short for penetration test. An authorised test of a computer network or system designed to look for security weaknesses so that they can be fixed.

Phishing
Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other forms of communication. Attackers will commonly use phishing emails to distribute malicious links or attachments that can perform a variety of functions. Some will extract login credentials or account information from victims.

Phreaking
Using a computer or other device to trick a phone system. Typically, phreaking is used to make free phone calls or to have calls charged to a different account.

Portable device
A small, easily transportable computing device such as a smartphone, laptop or tablet computer.

Proxy server
Server that acts as an intermediary between users and others servers, validating user requests.

Qualified security assessor (QSA)
A person who has been certified by the PCI-SSC to audit merchants for PCI-DSS compliance.

Restore
The recovery of data following computer failure or loss.

Ransomware
A piece of malicious software that encrypts or blocks access to data/systems, with a decryption key only being provided upon payment of a fee.

Red team exercise
An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by a hacker to attack or exploit vulnerabilities in a company's network.

Redundancy
Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.

Report on compliance (RoC)
Issued by a QSA if the audit of a merchant's systems have been found to be in compliance with PCI-DSS.

CYBER & DATA – **COMMON TERMINOLOGY**

Resiliency
The ability of a network to:
- provide continuous operation (i.e. highly resistant to disruption and able to operate at a lower level damaged);
- recover effectively if failure does occur; and scale to meet rapid or unpredictable demands (such as DDoS attacks).

Risk assessment
The process of identifying, analysing and evaluating risk.

Router
Device that directs messages within or between networks.

Salting
The addition of a unique, random string of characters to a password before it is hashed to make deciphering the password more difficult.

Sanitisation
Using electronic or physical destruction methods to securely erase or remove data from memory.

Screen scraper
A virus or physical device that logs information sent to a visual display to capture private or personal information.

Security control
Something that modifies or reduces one or more security risks

Secure file transfer protocol (SFTP)
A methodology for exchanging/transmitting files over the internet in an encrypted format.

Secure sockets layer (SSL)
An outdated protocol (replaced by TLS – see below) for transmitting private data via the internet by utilising cryptographic systems that use two keys to encrypt data.
Security information and event management (SIEM)
A security solution that provides visibility of a company's cyber security by aggregating alerts and logs generated by multiple sources and security assets (IPS, IDS, AV, etc.)

Security perimeter
A well-defined boundary within which security controls are enforced.

Self-assessment questionnaire (SAQ)
A self-assessment form used by smaller merchants to verify their compliance with PCI DSS.

Server
Computer that provides data or services to other computers over a network.

Smartphone
A mobile phone built on a mobile computing platform that offers more advanced computing ability and connectivity than a standard mobile phone.

Smishing
Phishing via SMS: mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website

Software-as-a-service (SaaS)
The delivery of software applications remotely by a provider over the internet; perhaps through a web interface.

Social engineering
The methods attackers use to deceive victims into performing an action, often including phishing, but also phone calls, fake LinkedIn accounts, etc. Typically, these actions are opening a malicious webpage or running an unwanted file attachment.

Spearphishing
A targeted phishing attack against a certain individual.

Spyware
Software that uses your Internet connection to send personally identifiable information about you to a collecting device on the Internet. It is often packaged with software that you download voluntarily, so that even if you remove the downloaded program later, the spyware may remain.

Supply chain
A set of organisations with linked resources and processes involved in the production of a product.

SQL injection
SQL is a computer programming language to tell a database what to do. An SQL injection is where that language is manipulated to instruct the database to perform a different task to what was intended.

Tablet
An ultra-portable, touch screen computer that shares much of the functionality and operating system of smartphones, but generally has greater computing power.

Threat
Something that could cause harm to a system or organization.

Threat actor
An individual, group, organisation, or government that conducts or has the intent to conduct detrimental activities. A hacker, essentially.

CYBER & DATA – **COMMON TERMINOLOGY**

Threat vector
The method that a threat actor uses to gain access to a network.

Transport layer security (TLS)
The successor to SSL (see above), and also a protocol for transmitting private data via the internet by utilising cryptographic systems that use two keys to encrypt data. Many internet browsers indicate a connection protected by TLS by displaying a padlock or security certificate near the website address field. Often still referred to as SSL.

Two-factor authentication
Obtaining evidence of identity by two independent means, such as knowing a password and successfully completing a smartcard transaction.

URL
Abbreviation for "Uniform (or Universal) Resource Locator." A way of specifying the location of publicly available information on the Internet. Also known as a Web address.

URL Obfuscation
Taking advantage of human error, some scammers use phishing emails to guide recipients to fraudulent sites with names very similar to established sites. They use a slight misspelling or other subtle difference in the URL, such as "monneybank.com" instead of "moneybank.com" to redirect users to share their personal information unknowingly.

Username
The short name, usually meaningful in some way, associated with a particular computer user.

User account
The record of a user kept by a computer to control their access to files and programs.

Virtual private network (VPN)
A method of connecting remote computers to a central network, allowing users to communicate or access the organisation's servers securely over the internet.

Vishing
The fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.

Wide area network (WAN)
Communications network linking computers or local area networks across different locations.

Water-holing (watering hole attack)
Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Whaling
Highly targeted phishing attacks (masquerading as a legitimate emails) that are aimed at senior executives.

Whitelist
A list of entities, IP addresses, applications etc. that are considered trustworthy and are granted access or privileges.

Whitelisting Software
A form of filtering that only allows connections to a pre-approved list of sites that are considered useful and appropriate for children. Parents sometimes use such software to prevent children from visiting all but certain websites. You can add and remove sites from the "permitted" list. This method is extremely safe, but allows for only extremely limited use of the Internet.

Worm
A form of malware that can replicate and spread without the need for human or system interaction. Think of it as malware on autopilot.

Zero-day vulnerability
A software bug, unknown to the developers, that hackers have detected and can exploit to adversely affect computer programs, data, additional computers or a network.

Zombie Computer
A remote-access Trojan horse installs hidden code that allows your computer to be controlled remotely. Digital thieves then use robot networks of thousands of zombie computers to carry out attacks on other people and cover up their tracks. Authorities have a harder time tracing criminals when they go through zombie computers.

If you still don't know your phishing from your vishing please contact us.

WRITTEN BY **MARK BRANNON**, CERT CII
COMMERCIAL DIRECTOR

Mark is a respected industry leader with over 17 years' industry experience in a variety of roles within the business insurance sector. He works across a wide spectrum of insurance product and policy development, delivery and optimisation for clients, including claims, insurer relationships, marketing and communications, and risk management. He specialises in addressing challenges business clients face, such as the potential for underinsurance and uninsured risks, responding to change, and anticipating future needs.

He currently works at Towergate as Commercial Director. Towergate is the UK's leading independent insurance broking platform and forms part of The Ardonagh Group, an international network of over 100 offices and 7,000 people which incorporates leading brands in both Lloyd's of London and global markets.

Read more advice from Mark at **www.towergate.com/mark-brannon-cert-cii-commercial-sales-broking-and-client-director**

www.towergate.com/additional-products/cyber-and-crime