TYSERS

Tell me more about...

CYBER INSURANCE

In a world of hyperconnectivity cyber-crime is an ever-increasing risk to businesses. Companies across all industry sectors, of all sizes and spanning all geographies are being impacted. Identifying your cyber risks and understanding how to manage and mitigate those risks is critical. This pack is designed to help your business start to assess your cyber exposures and begin to understand the valuable protection that insurance can provide, as part of a wider risk management programme.

Tell me...

MORE ABOUT CYBER INSURANCE

Tell me...

MORE ABOUT CYBER INSURANCE

Cyber insurance cover helps your business offset the costs of recovery after a cyber-related security breach, loss of data, a ransomware attack or a similar event.

Many businesses now consider data to be one of their most valuable assets, but it's an increasingly vulnerable resource.

A comprehensive cyber insurance policy will provide financial compensation for the direct costs incurred, and any liabilities payable, to third parties following a cyber-attack, a data breach or loss of data.

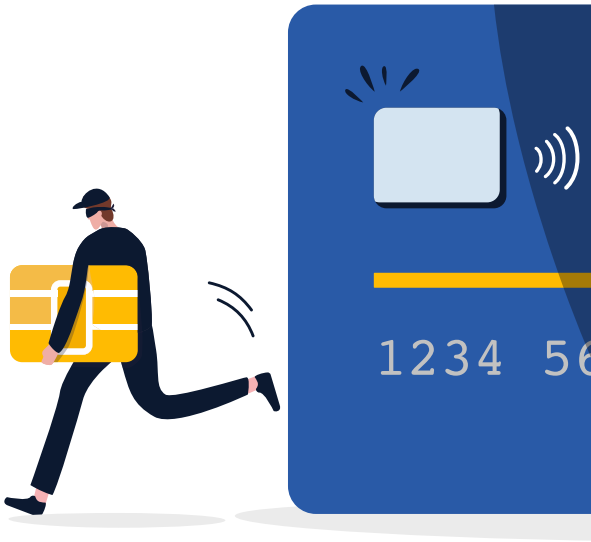
WHAT ARE THE RISKS?

Data Breaches

Data Losses

Cyber Criminals

Human error is the main cause of most cybercrime. In fact, according to the IBM Cyber Security Intelligence Index Report, 95% of cyber security breaches are primarily caused by human error. Human error is the unintentional action/s - or lack of action – taken by employees and users that cause, spread or allow a security breach to take place. In addition, data breaches can be caused by more sinister forces, where a business is the target of a malicious employee or sophisticated cybercriminals who gain unauthorised access to confidential data or sensitive information.



WHAT IS THE POTENTIAL IMPACT?

Financial Costs

Reputational Costs

A breach of security can lead to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by a business. Systems could be accessed, and data stolen, or business operations maliciously disrupted.

The UK GDPR introduced a duty on all organisations to report certain personal data breaches to the relevant supervisory authority.

Additionally, if a breach is likely to result in a high risk of adversely affecting an individual's rights and/or freedom, all individuals must be informed immediately, a process which can be costly.

A successful cyber attack or a data breach could cause major damage to a business. It could result in business interruption, financial loss and reputational damage, eroding clients' trust.

WHAT DOES CYBER INSURANCE COVER?

Cyber insurance is concerned with the loss of data and the impact of this. Loss of money due a cyber incident would be a crime claim which would need to be specifically added in to the cover or obtained separately.

1

FIRST PARTY

Similar to Material Damage and Business Interruption insurance policies, Cyber insurance covers your business's internal costs and losses to get you back up and running.

3

THIRD PARTY

Similar to Public Liability, Cyber insurance covers you against Third Party claims where an incident has financially impacted the Third Party.

!

INCIDENT RESPONSE SERVICE

A specialist incident response team will be provided to support you through any incident, they will provide guidance on how to best remedy the situation and advise on any steps you may need to take based upon their experience.

Many different insurers offer cyber insurance protection.

Policy wordings vary but, typically, include:

- Business Interruption. Compensation for loss of income, interruption expenses and additional work around costs following an interruption in service or computer system failure
- Costs of forensic investigation, restoration and notification following privacy breaches or loss of data
- Damages and defence costs following a privacy breach or loss of data
- Repair or replacement if cyber events damage your equipment
- Sums required to deposit a fund for payment of consumer claims
- Liability support if someone alleges you've transmitted a virus
- Extortion monies paid following a credible cyber threat
- Monies lost as a result of hacker theft if a crime extension is added to a policy
- Cover for damage, theft or destruction of data and computer programmes
- Media Liability for intellectual property infringement, resulting from the advertising of your services
- Help notifying regulators after an attack
- Fines, penalties, and defence costs arising from a claim by a regulator
- Costs arising from an internal investigation or enquiry commenced upon request from a regulator
- Help to recover your position where there's reputational damage
- Indemnity for losses incurred if your supplier faces a breach
- Costs of legal advice, IT Experts and other third-party consultancy costs incurred in response to a covered loss.

KEY CONSIDERATIONS WHEN PURCHASING COVER

The definition of an insured event

The definition of an insured event is the most important section of the policy wording.

The definition is in the policy wording and is the foundation of the coverage.

Definitions vary significantly between insurers which impacts the premium.

Usually, insurers with higher premiums will have a broader definition with more coverage.

Cover is usually provided for a failure of cyber security leading to a:

- Breach of personal or corporate information
- Loss or damage to systems and data.

Limit of Liability

Your potential exposure may be much greater than anticipated. Cyber incidents are often fast paced and costs can quickly escalate. We often experience claims where the limit of indemnity is insufficient due to the increasing costs of cyber experts within legal or forensic IT companies. We would recommend that you always discuss potential 'worse case scenarios' with your senior management team to ensure you are adequately protected.

Buyer Beware

When purchasing Cyber Insurance businesses must ensure they are fully conversant with all the policy exclusions and comply with any insurance subjectivities. Subjectivities and exclusions detail the terms and conditions you must follow to ensure you receive the coverage you need. It's an insurers way of guaranteeing your business upholds its systems and security to a particular standard. For example, if your systems are not sufficiently updated, tested, or patched you may find your insurance becomes invalid.


Tell me...
DOES MY BUSINESS NEED CYBER INSURANCE?

Tell me...

DOES MY BUSINESS NEED CYBER INSURANCE?

Find out here....

Many businesses mistakenly believe they do not need to purchase cyber insurance protection as they consider that they have a low-risk exposure.

However, if you answer yes to any of the following questions, we recommend you consider investing in cyber insurance to help protect your business.

Do you store any personally identifiable customer or employee data on your internal systems?

☐ Yes ☐ No

Anything 'personally identifiable' held on your systems presents a data risk. Examples of personally identifiable information include (but are not limited to):

- Social Security Number
- Email Address
- Date of Birth
- Passport Number
- Medical Records
- Driving Licence Number
- Home Address
- Passport Number
- Biometric Data

Do you have employees?

☐ Yes ☐ No

Most data breaches happen because of employee errors, such as clicking a phishing link in an email which can provide criminals with access to your networks.

Do you share customer or employee data with any third-party agencies?

☐ Yes ☐ No

Even when you pass data to a third party for processing you are still regarded as the Data Controller and may be held liable for any privacy breaches. For example, if you outsource payroll or any company processes to third parties you may be liable.

Do you gather any electronic payment information from customers or third parties?

☐ Yes ☐ No

Credit card details and payment information are highly attractive to criminals who can resell this information on the black market.

Does your business operate a website?

☐ Yes ☐ No

Material posted electronically, or in written format, may lead to copyright or trademark infringement, or defamation litigation. If the website is transactional, additional exposures include possible hacking or disruption of your business via denial-of-service attack.

Does your business use mobile devices?

☐ Yes ☐ No

Employees losing laptops or mobile phones, or having them stolen, especially with increased hybrid working is a key risk to your business.

Does your business allow employees to use personal devices to connect to your network?

☐ Yes ☐ No

These devices will not have the protection installed on company devices which could expose your network to viruses and/or malware.

Does your business store any information which would compromise your organisation if accessed (including customer or other information such as financial information, products design or intellectual property)?

☐ Yes ☐ No

A breach of confidential business information may lead to:

- Contractual liability
- Regulatory liability
- Other legal liability and costs
- Loss of future revenue
- Business disruption.

Would your business lose critical information should you experience a system failure or other network disaster?

☐ Yes ☐ No

Cyber insurance can cover network business interruption and may cover the costs related to restoring or recreating data due to a network security failure.

Do you allow employees or customers to access internal systems from remote locations?

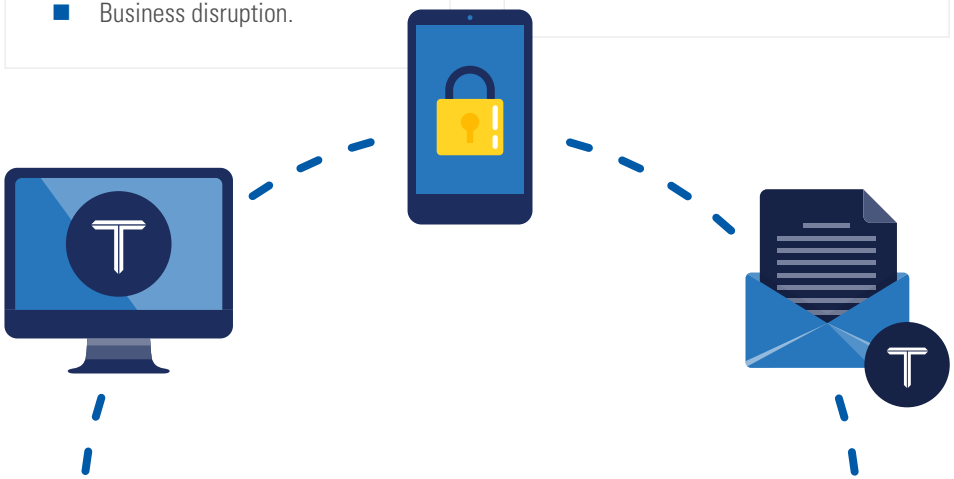
☐ Yes ☐ No

Your employees or customers could be connecting using an unsecured home wireless network or accessing their corporate accounts using unsecured public Wi-Fi.

Does your business store data in the cloud or use cloud-based services?

☐ Yes ☐ No

Cloud computing has revolutionised web-delivery technologies in the past few years. However, the major downside of cloud computing is cybersecurity threats. Cyber attackers have learnt to hack and attack cloud-based systems.



IMPORTANT NOTE

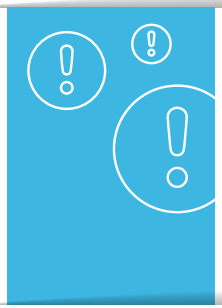
Purchasing cyber insurance does not remove the requirement for business owners to ensure their network and systems are secure and their day-to-day operations are protected.

Insurers will not pay claims if organisations have failed to take the appropriate steps to protect their own data networks against cyber security threats.

Insurance is just one element of a comprehensive cyber risk management programme. A robust cyber risk management programme should include the installation of reputable cyber security systems and following processes including, but not limited to:

- Regular security checks
- System updating
- Testing
- Training & education

EVERY CLIENT HAS A RISK



Incident Response

- What do you do in the event of an incident?
- Should and how do you pay a ransom request?
- Has information been stolen?
- Who, when and how do you report it to the ICO and clients?

First Party

Can you afford the costs of:

- Recollecting all lost information?
- Lost revenue during the outage?
- Paying a Ransom to release your system access?
- Obtaining new systems if permanently locked out?
- Notifying all potential customers?
- GDPR Investigations and fines?

Third Party

- Can you afford the cost of being sued by individuals and customers for the loss of their information?

Tell me...

HOW CAN CLAIMS OCCUR?

Tell me...

HOW CAN CLAIMS OCCUR?

Cybercrime takes many forms.

We've highlighted some examples of recent attacks, and claims settlements, experienced by our clients.

// Claims Example 1

RANSOMWARE ATTACK

A ransomware attack was launched on Client A, a major event producer, which immediately halted the client's ability to trade and left the business facing a ransom payment of hundreds of thousands of pounds. Undetected by Client A, the perpetrators had been infecting the client's systems for some time prior to lock down operations. When deployed, the ransomware encrypted all the client's files and back up files.

Specialist Consultants

The insurers were informed and appointed a team of specialist consultants to take control of the client's IT systems to prevent further virus spread and damage. Fortunately, the client's cyber insurance policy provided access to a team of expert IT anti-malware specialists who worked alongside the client's IT personnel.

Once the infected system was isolated, copies of back-up data could be examined within a stand-alone platform (sandbox) to check for viruses. After reviewing older back-up files some uninfected data was located and reconstruction of the client's data systems could begin.

When enough data was restored, the client started to trade again with minimal disruption. The perpetrators did not profit from their crime as the ransom payment was avoided. However, the insurer's costs for access to the team of IT specialist experts ran into thousands.

Additional costs included interruption of the business's activities, the service provider's contractual liability to provide an uninterrupted service to the client and notification and compensation for data lost during the attack.

// Claims Example 2

PAYMENT DIVERSION FRAUD/ BUSINESS EMAIL COMPROMISE*

Client B, a solicitor, made insurers aware of the loss of a payment of £100,000 from a client.

Insurer appointed a team of investigators, specialists in electronic fraud, who accessed the insured's systems and undertook a forensic search to understand how the thieves had hacked into the client's systems.

It was discovered that the hackers had gained access through a compromised mailbox. They had sent spoof email communications pertaining to be from the solicitor to divert the client's payment. The investigation revealed that the stolen funds had been transferred overseas and could not be recovered. Fortunately the insured had taken a cyber crime extension on their cyber policy therefore the insurer issued payment to the insured for the lost amount.

Forensic investigators were able to identify a rogue former employee who had been complicit in the hacking and who will face criminal charges.

TYSERS

// Claims Example 3

PAYMENT DIVERSION FRAUD/ BUSINESS EMAIL COMPROMISE*

Client C, a property management company, had arranged for a quote from a contractor for one of its customers. When final figures were agreed, the client received an email pertaining to be from the contractor, including bank details, which was passed to the client's customer to issue the payment. After the client was chased for the payment by the contractor, it became apparent that the payment had already been made and that the bank details were fraudulent. A hacker had gained access to the insured's (Client C's) mailbox and replaced the contractor's bank details with its own. The insured (Client C) changed its passwords and approached the bank for return of the funds, but only a small percentage of the lost amount was recovered.

The insured then involved its cyber insurer who, despite the late notification of the claim, issued payment to the insured for the unrecovered funds. Payment was possible because the client had taken the cyber crime extension on their cyber liability policy. The insurers' team of cyber specialists also assisted the insured with cyber security advice and training to help protect the company against future attacks.

*These types of email hijacks are also more generally referred to as a Man in the Middle Attacks as, in both cases, they involve the intervention of an unwelcome third party sitting between the client and their service provider.

// Claims Example 4

PHISHING SCAM
- LEADING TO THEFT OF CONFIDENTIAL DATA

Client D an international legal organisation, had made significant financial investment in IT support and therefore initially felt that a standalone cyber insurance policy would be an unnecessary additional cost to their business as they were confident their security was robust. However due to the Cyber exclusion on their PI policy and following consultation with their broker they decided to purchase a standalone policy with a £50k excess layer but decided upon a reduced policy limit of just £1m. (It is worth noting the indemnity limit on their PI insurance was £25m).

Six months after purchasing the cyber insurance the client suffered a data breach. Cyber criminals notified the client that they had stolen a large amount of data and they would release all their stolen client information unless they met a demand for a $10million ransom payment.

The ransom request was ignored, and the insured notified their broker of the 'circumstance' saying they believed they could manage the situation in-house , feeling there would be no need to notify a claim to insurers, as they felt confident, they would not exceed their £50k excess limit.

The criminals then released 56,000 of the stolen client files on to the darkweb and increased their ransomware demand declaring they would release yet more data if the ransom money was not paid in full. In response the company's IT, Legal and Management Teams had to spend a full day and night reviewing the information leaked to see if it was commercially sensitive and subsequently engage specialists and notify their clients appropriately.

It was at this point the client realised that their £50k excess would very quickly be exceeded and they submitted a formal claim to their insurer.

The hackers continued to threaten to leak more data on to the dark web. Charges from external consultants and specialists advisors to review the stolen information and contact all affected parties rapidly escalated into the millions.

This case clearly demonstrates how quickly indemnity limits can be exceeded as the costs of forensic investigations and responses can very rapidly escalate.

Tell me...

THE ANSWERS TO THE FAQ'S

Tell me...

THE ANSWERS TO THE FAQ'S

Here are the answers to some of the most commonly asked Cyber Insurance questions.

HOW MUCH WILL MY BUSINESS PAY FOR CYBER INSURANCE?

Costs will depend on several factors including (but not limited to):

Your industry sector

Certain industry sectors, such as the financial services sector, will pay higher premiums because statistics indicate they present a higher risk factor. For example, it is widely acknowledged that banking and financial companies are considered high risk, and research indicates that the following types of business are also considered particularly vulnerable to attack:

- Small businesses;
- Healthcare providers;
- Hospitality providers; and
- Legal firms.

The size of your business

Many insurance companies base their rates on the revenues a business earns, with larger revenues resulting in higher premiums. In addition, some insurers use the number of employees as a determining factor, with higher headcounts resulting in larger premiums.

The data you hold

Companies that don't hold or process much third-party information and have fewer data records are offered the lowest premiums. For example, small niche manufacturers with just a few customers.

Firms with large amounts of customer data but not sensitive or personal information would be considered mid-tier for premium charges.

In contrast, businesses that store sensitive information such a birth dates, financial records and social security information are charged higher premiums.

The level of cover you choose

Policies are generally available for small- to medium-sized business enterprises with cover limits between £100k and £5 million. However, significantly higher amounts of cover are available to larger firms with more complex cyber risk exposures.

Your security systems

Insurers are increasingly demanding evidence of effective cyber security defences, with many now requesting completion of a detailed cyber security questionnaire before accepting a new client. They will want to establish a clear picture of your business's internal security practices. This could include data loss prevention procedures, multi-factor authentication systems and encryption practices. Additionally, how often and quickly a business can spot, and patch, software vulnerabilities will be of relevance, and whether third-party vendors are used to monitor and assess security issues.

WILL MY PROFESSIONAL INDEMNITY/ PROPERTY OR OTHER BUSINESS INSURANCES GIVE ME SOME CYBER PROTECTION?

Your other insurance policies (such as Professional Indemnity, Property and Directors and Officers) may provide some level of insurance protection for cyber incidents, but the cover is likely to be very restrictive and limited.

As cyber-crime has escalated rapidly over the past decade, insurers expressed increasing concern about their possible claims exposure on non-cyber policies. Their concerns arose from the fact that policies had not been explicit about whether cyber was included or excluded. Insurers had remained silent on cyber and therefore as cyber crime increased so did their concern that they may be confronted with claims that they had neither underwritten or that a premium had been charged for.

In response, in 2019, Lloyd's of London mandated that all policies must be clear on whether cyber cover is provided.

The Lloyd's of London mandate prompted most insurers to apply exclusions for losses resulting from a cyber event.

However, if a cyber exclusion is not applied insurers must affirm the exact level of cyber cover provided. A broker will help you identify whether this is sufficient to cover your cyber exposure.

HOW MUCH CYBER INSURANCE COVER WILL I NEED?

The optimal amount of cyber cover for your business depends on how much it would cost to get your business back on track after a worst-case-scenario cyber-attack or data breach.

This approach helps to ensure you aren't left with insufficient funds in the event systems go down for an extended period, or criminals make a big ransom demand. Understanding the nature of cyber threats may help you to recognise the extent of risk to your business.

MY CYBER SECURITY ISN'T VERY GOOD, WILL INSURANCE HELP TO PROTECT MY BUSINESS?

No, you won't be able to rely on insurance to cover your losses if you suffer an attack due to poor security. If you fail to protect your business your insurance is unlikely to respond.

You will need to be able to demonstrate to insurers that you have taken steps to mitigate the risk of a cyber-attack and provide proof that you have the agreed security controls in place. Working with a broker will help you to get a better understanding of each insurer's requirements.

Tell me...

WHAT ARE THE MAIN CYBER SECURITY THREATS?

Tell me...

WHAT ARE THE MAIN CYBER SECURITY THREATS?

Cyber attacks are becoming increasingly sophisticated and will continue to evolve.

Here, we summarise some of the most widely recognised cyber threats and most utilised methods of attack.

INTERNAL THREATS

Employees

Recent research from the 2024 Insider Threat Report cites that 83% of organisations have experienced at least one insider attack, and 76% reported increased insider threat activity over the past five years.

Employees are also human, they make mistakes, and it's possible they could lose or mislay files containing data or could accidentally send data to the wrong address. Your business needs to ensure that system security and encryption make any mislaid data difficult to access.

In addition to deploying robust cyber security software and implementing robust processes and procedures, training and education is essential. You need to ensure that your employees remain vigilant and are able to detect cyber threats. For example, employees need to know how to create unbreakable passwords and how to identify potential phishing scams.

Restricting access will help manage the risk of employee breaches as this ensures that sensitive data is visible only to essential employees. When an employee exits your business, access to the company's systems and files must be removed.

EXTERNAL THREATS

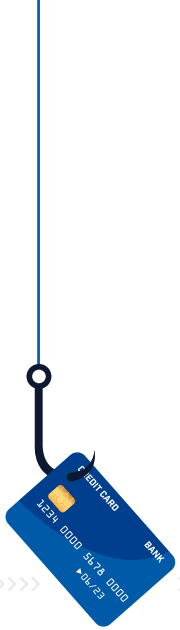
Denial of Service Attack (DoS)

A denial-of-service attack is when legitimate users are unable to access information systems, devices or other network resources. Often, DoS attacks are used by cyber criminals to hold companies to ransom and extort cash payments to release their systems.

Distributed Denial-of-Service (DDoS)

A distributed denial of service attack is a malicious attempt to make an online service unavailable to users by temporarily interrupting or suspending the services or its hosting server. It attempts to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding structure with a flood of internet traffic. Again, cyber criminals use this method of attack to disable business operations and extort payments in order to resume business as usual.

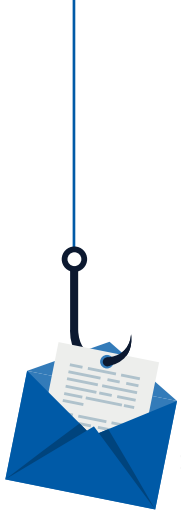
MORE EXTERNAL THREATS...



Man-in-the-middle Attacks (MITM)

A man in the middle (MITM) attack is a general term for when a perpetrator positions him/herself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

This method is used to extort money or extract and steal sensitive information.



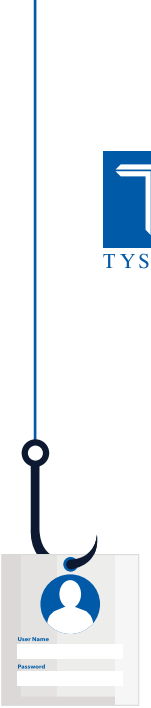
Social Engineering Attacks

Social engineering is the art of manipulating people, so they give up confidential information. Phishing is a type of social engineering, where criminals impersonate organisations via email, text message, or other means, in order to steal sensitive information or obtain money.

Malware & Spyware Attacks

Malware is malicious software, which can cause harm in many ways including:

- Locking your systems and devices and making them unusable (i.e. as part of a DoS and Ransomware attack).
- Stealing, deleting or encrypting data
- Taking control of your systems and devices with the aim of attacking other organisations.



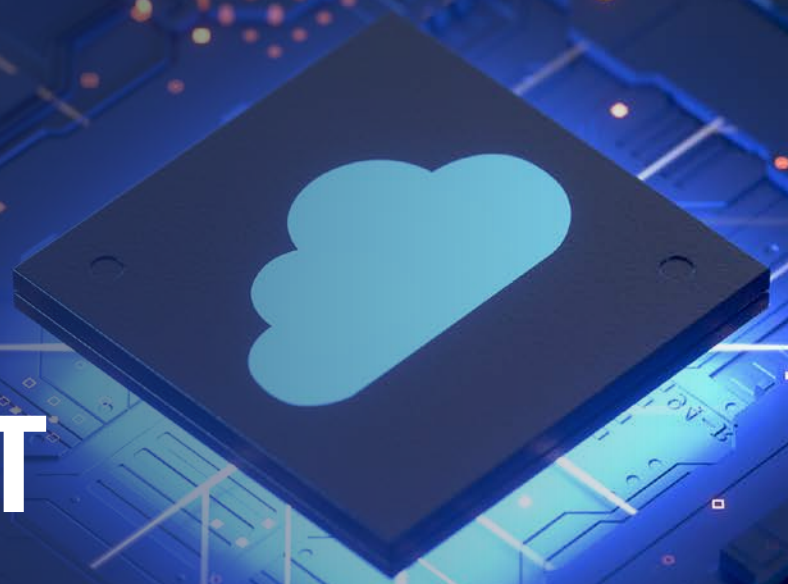
Password Attacks

A password attack is one of the most common forms of cyber-crime, it occurs when a hacker steals your credentials. During a password attack a criminal will aim to exploit weak or common passwords with the objective of gaining access to your systems.

TYSERS

Tell me...

MORE ABOUT CYBER BREACH RESPONSE SUPPORT



Tell me...

MORE ABOUT CYBER BREACH RESPONSE SUPPORT

Insurance will compensate you following a cyber-attack for costs such as:

- Lost revenue due to interruption of your business operations;
- PR management costs to protect against reputational damage;
- Third party liabilities e.g. cost of defending your business against legal action from external parties who claim their data was compromised as a result of your businesses failure to protect it; and
- Costs of notification and much more…

However, many insurers' policies offer significant additional value in terms of Cyber Breach Response Support which is an invaluable resource when dealing with cyber-attacks. These services can include crisis containment, PR and reputation management and independent legal advice. Many policies also offer the services of forensic investigation consultants and employee cyber training.

The benefits of the protection provided by a Cyber Insurance Policy extend far beyond recovering the costs incurred following a cyber-attack or breach. Cyber insurance can also improve your business's cyber security by raising awareness of any gaps and vulnerabilities in your existing practices.

CRISIS CONTAINMENT

When a crisis occurs, it's important to have the right support in place.

Many policies provide independent experts in crisis containment, who can advise next steps and implement a robust incident plan designed to limit damage to your business and reduce recovery time and costs. Typically, the team includes data recovery specialists and expert negotiators to help in recovering your data and assets from cyber criminals.

FORENSIC INVESTIGATION

Find the source and protect your business from future attacks.

Most comprehensive cyber insurance policies also cover the costs of forensic investigation consultants. These specialists will use forensic analysis to identify the point of entry and extent of potential system damages and will aim to recover data wherever possible. To reduce the risk of future attacks, consultants will also identify existing vulnerabilities in your current cyber security framework and advise how they can be fixed to improve protection.

PUBLIC RELATIONS & REPUTATIONAL MANAGEMENT

Reputation management experts to help you navigate adverse publicity.

In addition to the business disruption caused by a cyber-attack, you may also be faced with an onslaught of press and media enquiries, particularly if sensitive data has been compromised. As part of your policies protection, many insurers will cover the costs of a recommended PR company with extensive reputation management expertise. This will help you minimise damage to your business' reputation and brand during this difficult time.

Support can also be provided to prepare and issue communications notifying those individuals or third parties whose data has been stolen or compromised.

LEGAL ADVISERS

Expert legal advice following a breach or cyber-attack.

In a time of crisis, getting the right legal support is paramount. Many policies will cover defence costs for regulatory proceedings and the costs of independent legal specialists to evaluate your business' legal and regulatory obligations. Where there has been a breach of personally identifiable information or other consumer data, legal support may also include assistance with notifying regulators and data subjects.

ACCESS TO CYBER TRAINING

Training to help your business stay ahead of cyber criminals.

Cyber criminals are using increasingly sophisticated methods to damage or defraud businesses, including sophisticated phishing scams and malware. An IBM study reported that 95% of cyber breaches were caused by human error, therefore many policies offer cyber security training for your employees to help them identify cyber security threats and stay up-to-date on best practice.

TYSERS

Every business operating in today's world of hyper-connectivity is at significant risk from cyber-criminals, particularly businesses that store and process personal or sensitive data.

It's important to consider not only the level of compensation payable for direct financial losses but also to evaluate the critical resources policies could provide to your business at a time of crisis.

Tell me...

WHAT DOES THIS CYBER RISK JARGON MEAN?

Tell me...

WHAT DOES THIS CYBER JARGON MEAN?

Domain name system (DNS)

The domain name system is the address book of the internet. It acts as a directory containing:

- The contact's name (domain name), e.g., www.tysers.com; and
- The numbers associated with that name, i.e., the Internet Protocol (IP) address.

DNS hijacking

Also known as DNS poisoning or DNS redirection, it is the practice of intercepting web traffic and email communications with the objective of taking control. For example, your site could be cloned with the objective of stealing payment details.

Encryption

The process of converting information or data into a code, especially to prevent unauthorised access.

Endpoint

An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Examples of endpoints include desktops, laptops and smartphones.

Firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the internet.

Hackers

A hacker is a person skilled in information technology who uses his or her technical knowledge to achieve a goal or overcome an obstacle.

- **Black Hat hackers** are criminals who break into computer networks with malicious intent.
- **A white hat hacker**, or ethical hacker, is an individual who uses hacking skills to identify security vulnerabilities in hardware, software or networks.
- **A grey hat hacker** is someone who enacts a blend of both black hat and white hat activities. Grey hat hackers often look for vulnerabilities in a system without the owner's permission or knowledge. If issues are found, the hacker reports them to the owner, sometimes requesting a small fee to fix the problem.

Internet Protocol (IP) address

Every time you enter a web address in your browser, your computer uses your DNS to translate the domain name of the site in to a unique sequence of numbers (see DNS).

Malware

Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Multi-Factor Authentication (MFA)

MFA is an electronic authentication method in which a user is granted access to a website or application after successfully presenting two or more pieces of evidence to an authentication mechanism.

Penetration Testing

A method for gaining assurance in the security of an IT system by attempting to breach some, or all, of that system's security, using the same tools and techniques as a cyber criminal might.

Phishing

Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to the attacker, or to deploy malicious software onto the victim's infrastructure, like ransomware.

Ransomware

A type of malicious software designed to block access to a computer system until a sum of money is paid.

Salting

Password salting is a technique to protect passwords stored in databases by adding a string of 32 or more characters and then hashing them. Salting prevents hackers who breach an enterprise environment from reverse-engineering passwords and stealing them from the database.

Social Engineering

Social engineering is the art of manipulating people, so they give up confidential information. The types of information that criminals are looking for varies but, when individuals are targeted, it is usually with the purpose of tricking someone into giving them their passwords, bank information or access to a computer. The perpetrator will then secretly install malicious software that gives him or her access to passwords and bank information, as well as giving him or her control over the computer.

Spoofing

Spoofing involves individual/s impersonating a trusted contact or brand, pretending to be someone of trust in order to access sensitive personal information.

Structured Query Language (SQL) injection

An SQL injection is a code injection technique that has the potential to destroy a database. SQL injections attack data-driven applications, making it possible to carry out malicious SQL statements and attack a database.

Tokenisation

Tokenisation, when applied to data security, is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value. It can be used in a database or internal system without bringing it into scope.

Although the tokens are unrelated values, they retain certain elements of the original data —commonly length or format—so they can be used for uninterrupted business operations. The original sensitive data is then safely stored outside the organisation's internal systems.

Virus

A type of malware, a computer virus is a malicious piece of computer code designed to spread from device to device.

TYSERS

tysers.com