HISCOX

Hiscox cyber claims report 2018

Hiscox, the international specialist insurer, is headquartered in Bermuda and listed on the London Stock Exchange (LSE:HSX). There are three main underwriting divisions in the Group – Hiscox Retail (which includes Hiscox UK & Europe, Hiscox Guernsey, Hiscox USA and subsidiary brand, DirectAsia), Hiscox London Market and Hiscox Re & ILS. Through its retail businesses in the UK, Europe and the US, Hiscox offers a range of specialist insurance for professionals and business customers, as well as homeowners. Hiscox underwrites internationally traded, bigger ticket business and reinsurance through Hiscox London Market and Hiscox Re & ILS. For more information please visit www.hiscoxgroup.com.

Introduction

From payment diversion fraud to cryptojacking...

Managing the cyber risk
Cyber insurance might seem like a relatively new product but, at Hiscox, we have been providing businesses with cyber protection for nearly 20 years and we have dealt with over 1000 cyber related insurance claims from businesses over the past 12 months alone. The single biggest cause of a claim was ransomware – where a business' computer system is effectively put out of action by a hacker until a ransom is paid. Analysis from across the market suggests that this tactic is on the decline as people and businesses become more aware of the threat after the Wannacry and Petya attacks of 2017, although we are still seeing ransomware related insurance claims in 2018.

Another central cause of cyber related claims seen over the last year was through payment diversion fraud; where a criminal manages to fraudulently persuade an organisation to pay them rather than a supplier. We believe this may be because incidents of this type require relatively low levels of technical sophistication, where attackers often just use their phones for simple social engineering attacks, or create spoofed email addresses to lure in potential victims.

The rise of cryptojacking
What these tactics suggest is that while cyber criminals might still be very interested in stealing and using confidential and personal data for financial gain, there are now more direct ways to profit from cyber crime. Cryptojacking – where criminals use the processing power of a business' computer systems to surreptitiously mine for cryptocurrency – is the latest of these trends and we explore its impact later in this report.

The examples in this report give a broad overview of the range of claims we've seen in the last year, spread across different sizes of company, industries and geographies. The key learning is that no business is immune from the growing cyber threat.

We've seen that attackers are evolving their methods, targeting both the better protected perimeter of a company's network and the softer underbelly – their staff. Employee error has emerged as a key risk and we see examples of attacks related to phishing within the report. The threat goes beyond this to include drive-by website infections and the danger of staff sending confidential data insecurely or losing unsecured mobile devices. Businesses must ensure their staff are equipped to deal with the risk and employee training is key.

Responding to the threat
In each of the examples we highlight, cyber insurance went beyond the promise to pay and played a crucial role in responding to the threat. It gave affected businesses fast access to a range of experts including experienced cyber claims handlers to support them through the incident, forensics specialists to remediate the threat, and legal and PR teams to help prevent reputational damage. Our aim is to get our customers back on their feet as fast as possible whilst still providing financial support for any associated loss of income.

In a cyber insurance market expected to be worth US$36 billion by 2027 (compared to US$3.2 billion today), this Hiscox cyber claims report – the first in a series of cyber reports and related material we will be producing – is intended to help our customers and the wider business community better understand current and emerging cyber risks; how they can help reduce the risk to their organisation; as well as illustrating how insurance can form part of a cyber risk management strategy.

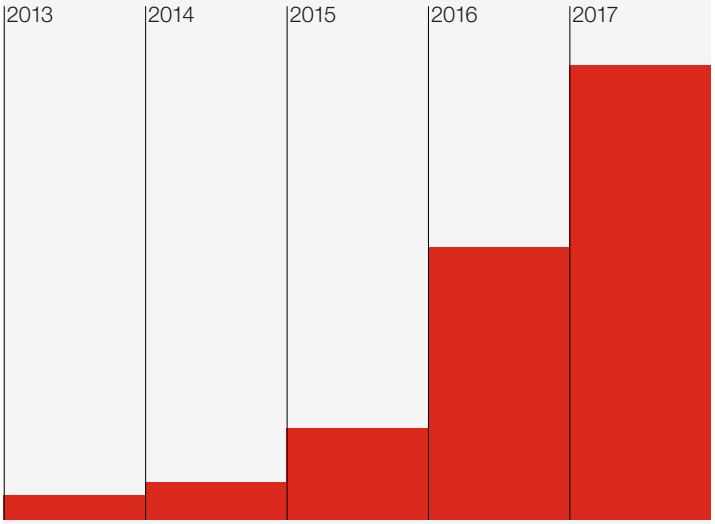
Gareth Wharton
Cyber CEO
Hiscox

Cyber claims by numbers

Over 1,000 claims in 2017

Claims count growth

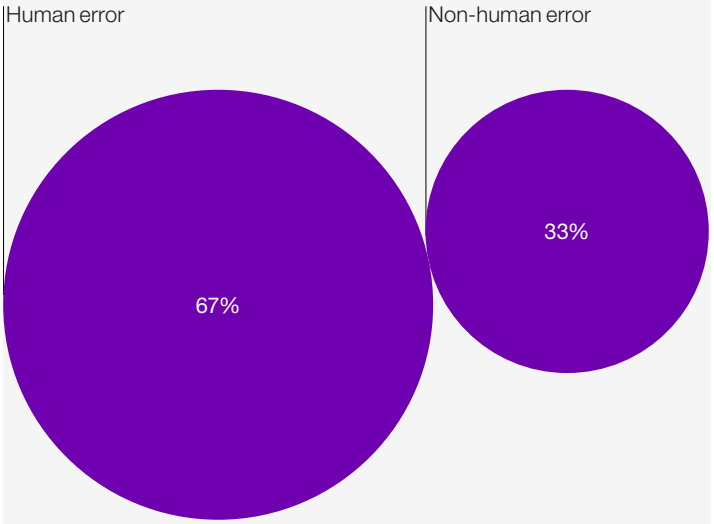
Across all Hiscox territories



Since 2013, the rise in claims against the cyber insurance policies we have issued has risen by more than 1,700%. This is from a relatively low base but is a good indicator that businesses of all sizes and in all geographic regions are experiencing far more activity related to the cyber threat than five years ago. This is resulting in far greater potential for financial and reputational loss.

2017 Hiscox claims

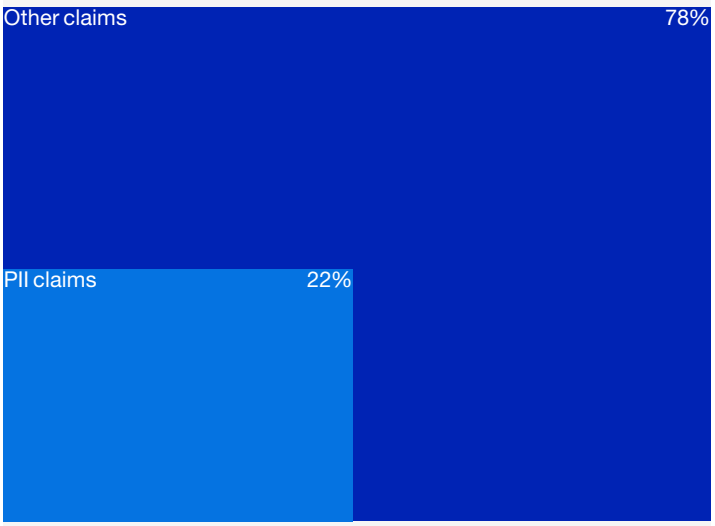
UK retail



Over two thirds (67%) of all claims involve an element of employee error. Examples include employees clicking on malicious emails, visiting harmful websites or simply being negligent in losing devices. It is vital that business' not only invest in technology, but also process and people, ensuring that their staff are an effective first line of defence.

2017 personally identifiable information (PII) claims

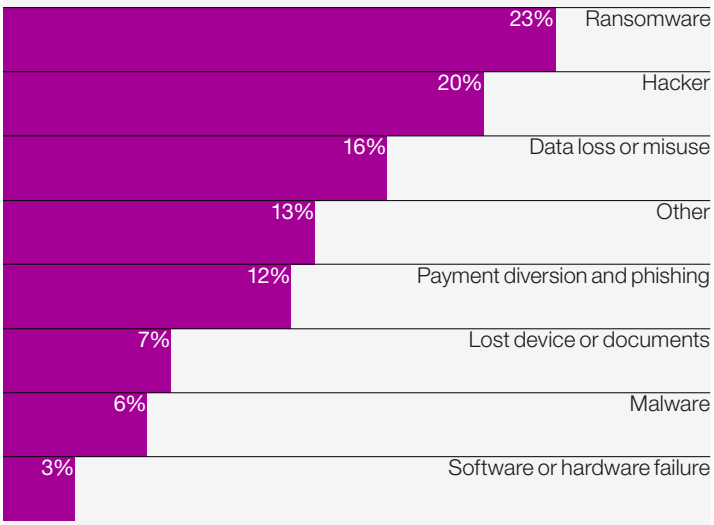
UK retail



Nearly a quarter of the claims (22%) in the UK involved the loss or misuse of PII. Given the tightening of regulations, incidents of this kind could become more costly both financially and from a reputational perspective. Despite this, 78% of claims did not include loss or misuse of data, presenting a risk even for business' that hold little or no PII.

2017 cause of claims

Across all Hiscox territories



While ransomware was the most prevalent cause of claims in 2017, the graph above illustrates the wide range of attacks that businesses have to protect themselves from. Some of these threats are external, some are internal and some are accidental. Combined this shows the need for a cyber defence strategy that encompasses people, process and technology.

Spotlight on SME cyber claims

Ransomware still on the rise

As in 2016, ransomware remained the largest source of cyber-related insurance claims for 2017, largely due to the low barrier to entry for hackers, ease of deployment and the prospect of a decent return on a minimal investment. Ransomware usually involves human error, where mistakes by employees also lead to many phishing and social engineering attacks. Below are four anonymised examples of actual cyber insurance claims we have dealt with over the last 12 months, three of which involved an element of human error.

No ordinary case of ransomware

Sector	Technology
Turnover	£10m – £50m
Claim cost	£370,000

Background

Our insured became aware that its IT systems had been compromised when a number of folders were encrypted and a ransom demand was made. The hacker had determined the identity of the administrator of the company's network and then used a brute force attack to identify their password.

Using the administrator's credentials to remotely access the company's systems, the attacker was able to obtain further credentials giving them even greater access. PII and commercially sensitive data (contracts, bank account details etc.) were compromised.

Hiscox response

The company contacted us and we immediately arranged for a data breach coach – a specialised role to help companies respond to a breach – and an IT forensic firm to investigate the extent of the breach, resecure the company's network and understand its contractual and regulatory notification obligations. We also engaged a PR agency to advise the company on its communications with the press and customers.

A notification was made to the local data protection regulator as well as the data subjects affected and customers. The swift action taken resulted in the regulator taking no further action.

Lessons learned

- The attacker tried a large number of password combinations (usually in the thousands) until finding the correct one. To protect against against this sort of attack, good user account management is critical, for example locking out accounts after a large number of failed login attempts.
- The UK's National Cyber Security Centre (NCSC) has good advice on this subject and recommends that businesses:
  - allow around ten login attempts before the account is frozen;
  - put in place protective monitoring. A powerful defence against brute force attacks and offers a good alternative to lockout or throttling;
  - give administrators, remote users and mobile devices extra protection such as two-factor authentication;
  - ensure that administrators use different passwords for their admin and non-admin accounts;
  - consider implementing two-factor authentication for all remote accounts.

Revenge DDoS attack

Sector	Financial services
Turnover	£10m – £50m
Claim cost	£130,000

Background

A loan aggregator company suffered a series of DDoS attacks – a cyber attack that aims to bring down services by bombarding the networks with more traffic than they can handle – which crippled its website for several days, leaving it unable to trade.

Hiscox response

A police investigation revealed that the attacks were by a disgruntled employee. We covered the costs of the insured engaging its IT contractors to restore its systems. The company also suffered a very significant business interruption loss as a result of the breach.

Lessons learned

- Organisations that depend on their customers being able to access their internet based services should consider purchasing a DDoS mitigation service. These services filter out unwanted traffic before forwarding on legitimate requests to the appropriate website.

A large restaurant bill

Sector	Food services
Turnover	£1m – £10m
Claim cost	£20,000

Background

A ransomware attack encrypted a restaurant's entire server, impacting its point of sale registers and meaning it was effectively unable to trade.

Hiscox response

Having exhausted all other options, it was clear that the most effective way to restore the restaurant's systems was to pay the ransom.

We covered the cost of the ransom, together with the associated IT costs of applying the decryption key and ensuring that the insured's business was back up and running. We also engaged a breach coach to confirm whether any PII had been compromised. In addition to these costs, we covered the business interruption suffered by the restaurant as a result of being unable to trade.

Lessons learned

- By helping staff recognise the style of potential phishing emails, or what to look for in email senders' details to help identify suspicious looking emails, companies can significantly reduce the risk of phishing attacks.
- It is also important to ensure that good back-ups are in place. These should be regularly tested and done through a system that is not connected to the main network, for example on a hard drive.

A costly phishing trip

Sector	Financial services
Turnover	£50m+
Claim cost	£230,000

Background

An employee at a financial services agency fell victim to a phishing incident in which a spoof email from one of the company's senior managers requested that the employee wired £230,000 to a specified bank account. Believing the request to be genuine, the employee issued the fraudulent wire and both the agency's bank and the receiving bank were unable to recover the funds. The email was actually from a Gmail account created to imitate the senior manager's genuine address.

Hiscox response

On realising what had happened, the agency called us and we immediately engaged a data breach coach and IT forensics to confirm whether there had been any breach of the insured's systems or whether PII had been compromised.

We reimbursed the money lost within a month of notification while it was confirmed that no breach of data had occurred so there was no need for any notification.

Losses for payment diversion fraud are covered as standard under our US cyber insurance policy and can be offered as an additional cover in other territories.

Lessons learned

- Better staff training remains important here in order to help staff identify potential phishing emails
- It is important to check email addresses carefully before taking action. Companies can help their employees by including an identifier on all emails that are received from external sources, such as including the wording 'email originates from outside the organisation' or similar.
- A change of culture can also make a big difference in mitigating this type of threat. Senior management should look to create an environment where employees are more likely to do the 'right thing' rather than simply satisfy an 'urgent' request from a client or a senior colleague. Ideally, wire transfer requests to new or modified accounts should be verified by calling the other party on a predetermined phone number – one that they already have, not one that may be in a phishing email, as hackers often give bogus numbers.

What next: cryptojacking

More lucrative, less effort for criminals

Criminals are starting to move away from obvious and invasive ransomware attacks to a more stealthy cyber crime; cryptojacking. According to Symantec, instances of cryptojacking rose 8,500 percent in the final quarter of 2017. Once a hacker has access to a compromised computer system, instead of downloading a ransomware payload that encrypts the victim's files, the cryptojacking attack will install 'mining' software. This sits in the background and uses spare processing resource within the victim's machine or office server environment and quietly mines crypto-currency for the hacker. Whilst we have seen cases where the mining software has been so invasive that the victim's machines can no longer complete their intended task, our view is that the more savvy hackers will use a smaller percentage of computer processing capacity allowing their activity to remain undetected and therefore earning more in the longer term.

An IT firm falls victim

Sector	Technology
Turnover	£50m+
Claim cost	£70,000

Background
A technology company noticed that a piece of malware had been installed on one of its servers.

Hiscox response
We immediately instructed an IT forensics firm to investigate what the malware was doing and how it had been installed on our insured's systems. The server contained a substantial amount of PII and so we also investigated whether there was any wider breach or risk that PII had been compromised.

Given the potential gravity of the breach, we also instructed a breach coach to manage the investigation. The investigation confirmed that the malware was mining, but fortunately nothing more than this and there had been no wider breach.

Advertising for Bitcoin

Sector	Marketing
Turnover	£0 – £1m
Claim cost	£40,000

Background
A PR company noticed a problem with its emails. Its regular IT contractor investigated and concluded the most likely cause was malicious activity. The insured contacted us and we deployed an IT forensics team who were quickly on site to investigate and confirmed the insured had indeed been the victim of an attack.

The PR company's IT systems had been infected with crypojacking malware to mine for cryptocurrency. They also confirmed that the hackers who deployed the malware had accessed the insured's systems and that PII was potentially compromised.

Hiscox response
After investigating the extent of the breach, the IT team removed the malware and plugged the gap in the PR company's security which had allowed the breach. We then engaged legal counsel to advise the insured on its notification obligations, and then arrange the notification of the regulator and relevant data subjects.

Lessons learned

In both these cases – alongside the standard advice regarding good password management and regularly updating software to ensure it is fully patched – organisations can also use server monitoring software to track the key metrics of servers such as processor, memory, network and disk usage. Over time, the monitoring software will create a baseline from which thresholds can be set. This can be a useful way to track server outages, and it can also detect if unusual levels of network traffic are detected, helping to indicate when data is being exfiltrated. If processor utilisation is higher than expected for extended periods, this could also indicate that cryptomining malware is running on a system.

Glossary of terms

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

Advanced persistent threat (APT). A type of high-level targeted attack carried out by an attacker who has time and resources to plan an infiltration into a network. These are usually seeking to obtain information, proprietary or economic, rather than simple financial data. APTs are persistent in that the attackers may remain on a network for some time and usually bypass regular security controls.

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

Anti-malware/anti-virus. Software which uses a scanner to identify programs that are or may be malicious.

Attack surface. All of an organisation's internet-facing assets including both hardware and software. A larger number of such assets yield 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.

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

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

Botnet. A collection of infected computers or internet connected devices that are remotely controlled by a hacker and report to a command-and-control server.

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

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

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

Cookie. Files placed on your computer that allow websites to remember details.

Cryptojacking. The unauthorised use of a target's computer systems to mine cryptocurrency.

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.

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

Distributed denial-of-service attack (DDoS). An attack which prevents users from accessing a computer or website by overwhelming it with requests and/or instructions, often carried out using a botnet.

Domain name system (DNS). The phone book of the internet. It allows computers to translate website names, like 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.

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

Encryption. The process of converting information or data into a code, so that it is unreadable 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.

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

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.

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

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).

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

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.

ISO27001. An international standard that describes best practice when it comes to information security risk management.

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

Malware. A general term for malicious software. Malware includes viruses, worms, trojans and spyware. Many people use the terms malware and virus interchangeably.

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

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

Patches. Software and/or 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 that governs how companies accepting payments by credit or 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 four at the bottom end to level one 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 brands (Visa, Mastercard, American Express, JCB and Diners) and supported by an 'advisory board' made up of representatives from major partners (retails, processors, banks, etc.).

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

Phishing. The fraudulent practice of sending emails purporting to be from reputable sources in order to induce individuals to perform particular actions, such as revealing information, transferring funds, or opening attachments or links.

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

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

Ransomware. A piece of malicious software that encrypts or blocks access to data or 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.

Remote desktop protocol (RDP). A methodology that allows users to remotely connect to computer systems over the internet.

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.

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

Rootkit. A piece of software that hides programmes or processes running on a computer.

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

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

Secure sockets layer (SSL). An outdated protocol (replaced by TLS) 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).

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

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.

Spoofing. When the sender address of an email is forged for the purposes of social engineering or phishing.

Spyware. Software that permits advertisers or hackers to gather sensitive information without your permission.

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.

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

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

Transport layer security (TLS). The successor to SSL 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.

Trojan. Malicious programs that pretend to be legitimate software, but actually carry out hidden, harmful functions.

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

Virus. Malicious programs that can spread to other files.

Vulnerability. Bugs in software that hackers exploit to compromise computers.

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

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 computers, programs, data or a network.

Zombie (aka bot). An infected computer that is remotely controlled by a hacker. It is part of a botnet.

Hiscox Ltd

4th Floor
Wessex House
45 Reid Street
Hamilton HM 12
Bermuda

T +44 (0)20 7448 6000
E enquiries@hiscox.com
hiscoxgroup.com

19079 7/18