P4P Compliance Management Limited

Simplifying Compliance

Introduction to Cyber Security

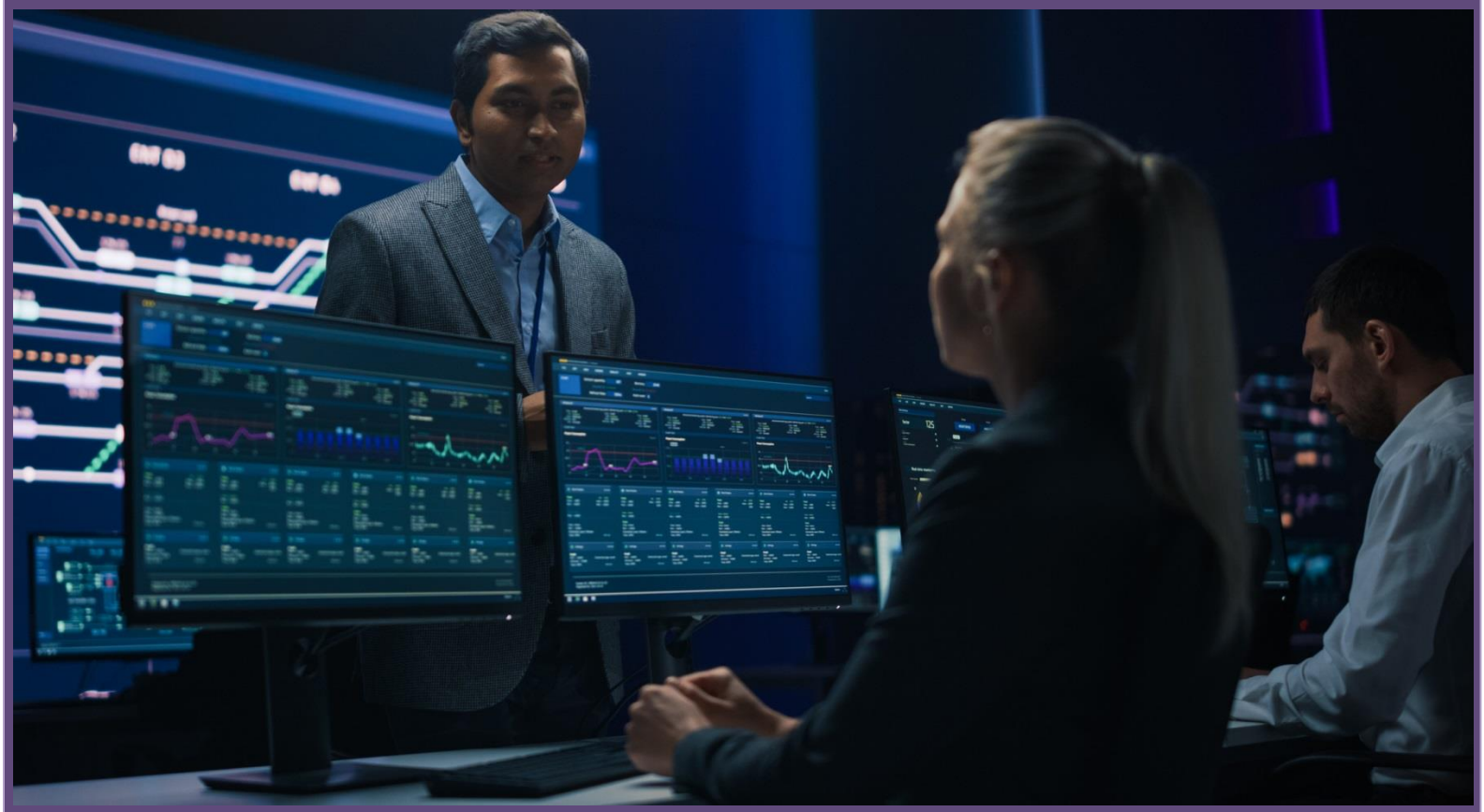


Table of Contents

Introduction

This Guide has been produced to provide an overview of Cybersecurity to help individuals and organisations develop and implement a Cybersecurity strategy.

The purpose for this guide is to explain in simple terminology (no complicated jargon) the basic fundamentals of Cybersecurity.

When using computers, tablets or smartphones for internet banking, online shopping, sending and receiving emails or social media, it is vital to take necessary steps to prevent hackers or cybercriminals from getting hold of your data.

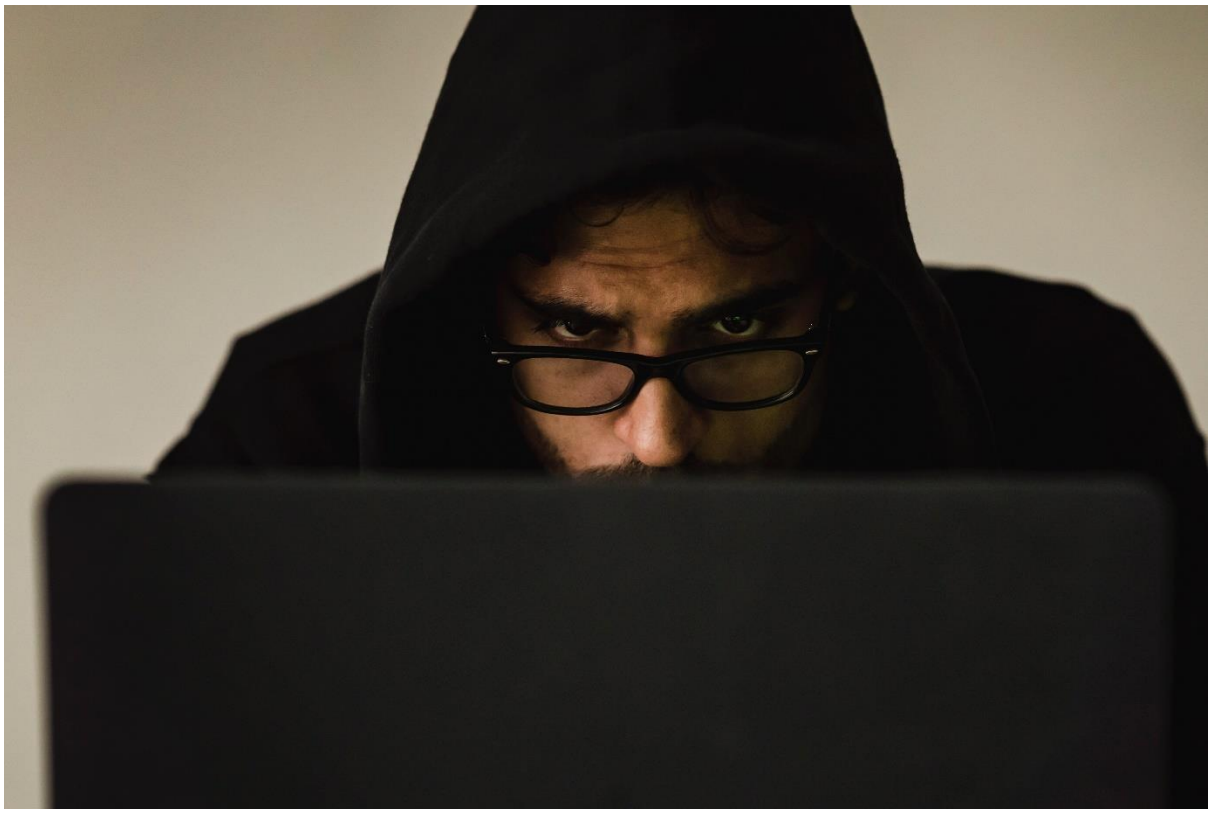
We all spend more time online, which means more opportunities for cybercriminals to carry out cyberattacks by targeting people and businesses using:

- email and website scams
- malware software that can damage your device or let a hacker into your computer system

If hackers get into your device or accounts, they could access your money, your personal information, or information about your organisation.

Cybersecurity is all about protecting the devices we use and services we access while online, either at home or work and preventing unauthorised access, theft of valuable information and sensitive data or damage caused by cyber-attacks.

Who are Cybercriminals?



Not all cybercriminals are hooded young male individuals (black hats), but a varied group of malicious attackers young, and old, men and women, from all over the world driven by a range of devious motives.

Their unofficial mascot is the image of Guy Fawkes, known as hackers often working in gang's and using computer systems to gain access to business and personal information for malicious and exploitive purposes.

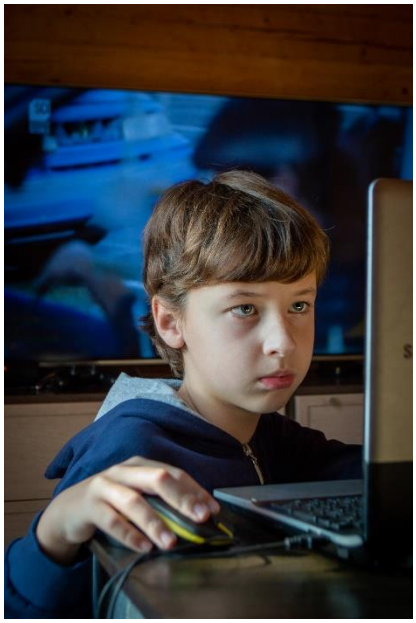
Cybercriminals are difficult to identify due to the cunning and shady security measures they use to protect their identity.

The growth of the cybercriminal network globally is due to the increased use of the internet opening a window of opportunity for financial incentives, has created a number of different types of cybercriminals, many of which present a major threat to individuals, organisations and even governments.

Types of Cybercriminals

Organisations today need to be capable of identifying potential hackers and understand the techniques cybercriminals use to prevent cybercrimes.

Cybercriminals come in different forms, from novices to serious harmful horrible characters.



Script Kiddies
These less experienced malicious hackers are usually only able to attack very weakly secured systems, using existing software developed by others to launch hacking attacks.

Hacker Groups
Groups of organised criminals who unite to carry out cyberattacks in support of political causes - hacktivists, terrorists, or even state-sponsored hackers.
They typically target entire industries or specific organisations that they feel don't align with their political views or practices.

Derive from the colour coding scheme found in 1950s westerns, where the bad guys wore black hats, and the good guys wore white.

Black Hat
Unethical criminals that break into computer networks to hold computers hostage.
Releasing malware to destroy files, steal passwords, credit card numbers, or other personal information.
Many Black Hat hackers started as novice "script kiddies" trained up to work for sophisticated criminal organisations.

White Hat
Ethical security hackers, using their programming skills for good lawful reasons. Companies hire these good guys to stress-test their information systems (network penetration tests) to discover vulnerabilities and uncover security failings in organisation computer network systems to help safeguard businesses from dangerous hackers.
They run deep scans for malware, using methods Black Hats would use, and even try to fool staff into clicking on links that lead to malware infestations.

Gray Hats
Somewhere between white and black lies the ugly Gray Hats.
These hackers like to believe they're doing something good for companies by hacking their websites and invading their networks without permission to look for vulnerabilities. They might inform an organisation that they have been able to exploit their system and subsequently ask for a fee to fix it.
In most cases, a Gray Hat's real intention is to show off their skills and gain publicity for what they consider a contribution to cybersecurity.

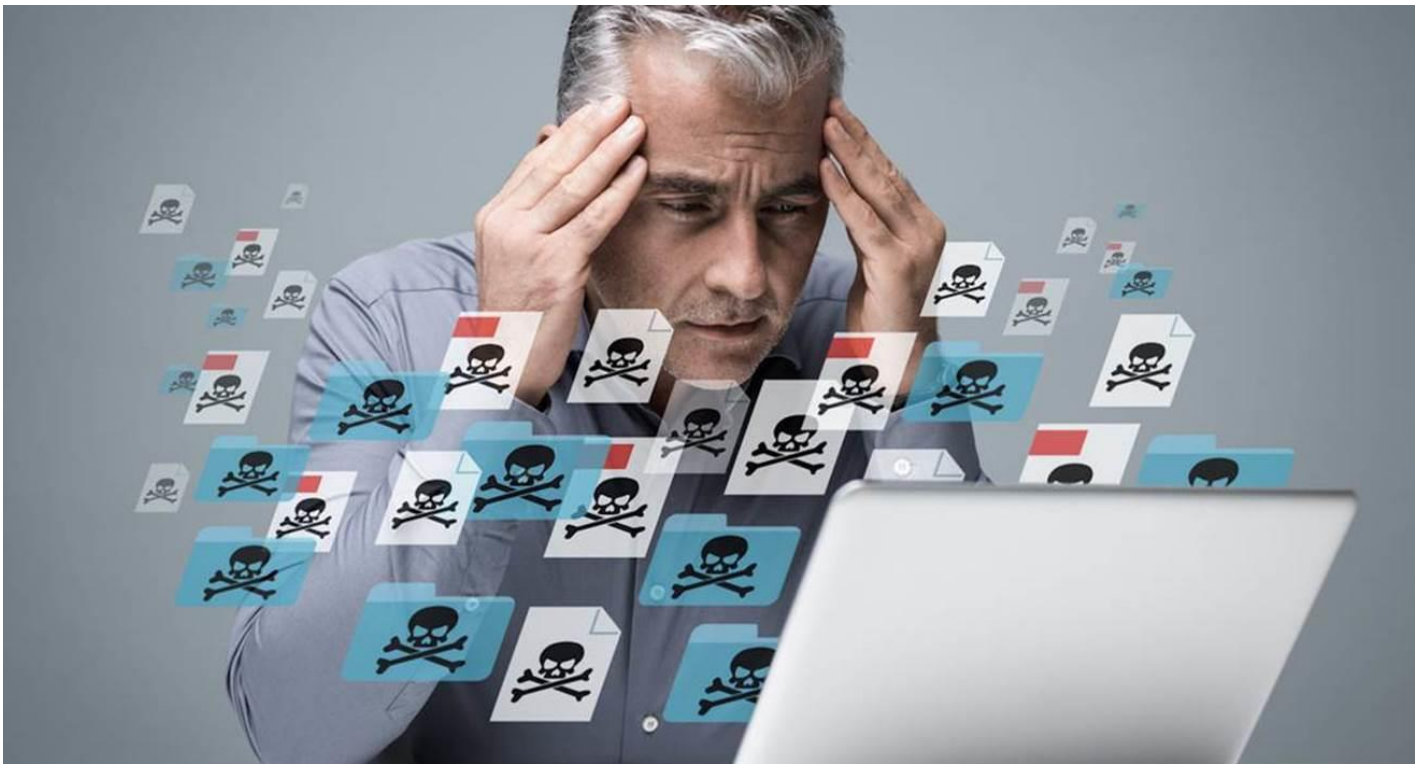
Internet Stalkers
People who maliciously use the internet to stalk or harass any individual, group or organisations (Cyberstalking) to acquire personal data. This type of cybercrime is through social media networking platforms and malware that tracks an individual's computer activity with little or no detection.
A stalker may be an online stranger or a person whom the target knows, motivated by a desire to control, intimidate, or influence a victim.

Scammers
Are unscrupulous people that try to steal your money by email.
The most common types are fraudsters pretending to be from HMRC or your bank to get your bank account number or credit card details.

Phisher
Phishing is malicious activities accomplished through human interactions (social engineering). These crooks use psychological manipulation to trick you into making security mistakes, give away personal sensitive or confidential information or get you to click on links to malicious websites or open attachments that contain malware.

Malicious Insider
They may only be 20% of the threat but produce 80% of the damage and are considered the highest risk attackers.
Disgruntled employees become hackers with a particular motive to commit cybercrimes.
Dissatisfied employees only option was to go on strike against employers, however with the advancement of technology and the majority of work now done on computers, aggrieved employees can misuse or steal sensitive information they have access to, on an organisation network.

Types of Cyber Attacks



There are many ways cybercriminals hack into a website or computer networks. Below are some of the most common methods used.

Malware
A type of malicious software whose intent is to exploit a user's vulnerability when they click on a dangerous link or open an email attachment that subsequently installs malicious software on their computer.
Once infected, malware can obtain information by retrieving data from the hard drive disrupting the computer system and making it inoperable.

Types of Malware attacks:

Viruses
A virus is a specific type of malware that infect software applications and computer files and then self-replicates by inserting its code into other programs in the computer system.

Trojan Horse
Typically hidden in an email from someone you know and click on what looks like a legitimate link, application or attachment. Once downloaded and opened it installs malware and takes control of your device.

Worms
Arrive as attachments in spam emails to send a copy of themselves to every contact in the infected computer email list, overloading email servers.
Once opened, worms are automatically downloaded and installed into the computer system, infecting the device without the user's knowledge.
Worms can modify, delete files, steal data, or inject additional malicious software onto a computer.

Ransomware
Ransomware locks and encrypts files on a victim's computer or device holding them hostage, and keeping you from your documents, photos, and financial information. Those files are still on your device, but inaccessible.
In many cases, the victim is threatened into paying a ransom for fear of the cybercriminal publishing or deleting the data. However, paying the ransom doesn't ensure access will be restored.

Spyware
A computer program installed on a device that collects information about users, their systems or web browsing patterns, and then sends the information to a remote user. The attacker uses the information collected for blackmailing purposes or to download and install other malicious programs.

Phishing
A common attack that sends an official-looking but fraudulent email to large numbers of unsuspecting random recipients that appears to come from a trusted sender.
The more emails they send, the more likely they are to find a victim who will open them.
The emails contain links that take them to malicious websites that are often clones of legitimate ones. Once on the landing page, malware is downloaded or the page contains credential-harvesting scripts.
Or the email contains malicious attachments, which can have enticing names, such as 'INVOICE', when opened it installs malware on victims' device.

Types of Phishing attacks:

Spear Phishing
Targeted at specific companies and or high-profile individuals by luring them into surrendering information or clicking a link that installs malware. The email may appear to come from someone you know such as an employee in a position of high authority

Man-in-the-Middle (MitM)
An attacker exploits security vulnerabilities in a network, such as an unsecured public Wi-Fi. The criminal intercepts a two-party transaction by inserting themselves in the middle and interrupting traffic to steal data.
This kind of attack is difficult to detect, as the victim thinks the information is going to a legitimate destination such as a popular online shop.

Whaling
Also known as CEO fraud, cybercriminals pretend to be senior executives, directly target other senior or important individuals at an organisation.
Via email or website spoofing, they attempt to steal money, sensitive information or gaining access to computer systems for criminal purposes.

Business Email Compromise (BEC)
These emails can take the form of ‘urgent’ requests and appear to be from senior staff, such as the CEO. Often using tactics to fool other staff members into disclosing confidential business information.

Pharming
Domain Name System (DNS) cache poisoning captures user credentials through a fake login landing page.
By exploiting vulnerabilities in a network system it attacks by impersonating and redirect a website’s traffic to the malicious fake website and capturing user credentials.

Clickjacking
Attackers place malicious clickable content over legitimate buttons on a website. Typically, an online shopper might think they are clicking a button to make a purchase but will instead download malware onto their device.

Password Attack
Passwords are the most widespread method of authenticating access to confidential and secure information, making them an appealing target for cyber attackers.
These attackers use countless methods to identify passwords to deceive and gain access to a password database, including testing computer network access to obtain unencrypted passwords.
Attackers often guess a user’s password by using a “brute-force attack”, a program that tries all the possible variants and combinations of information to guess the password.
Another familiar method is the "dictionary attack" when the attacker uses a list of common passwords to access a persons computer and network.

Rootkits
Commonly spread through email attachments and downloads from insecure websites. Hidden inside legitimate software, when installed the rootkit installs itself, gaining remote control and administrator access to a system, giving the attacker the ability to steal passwords and retrieve critical data.

Internet of Things (IoT) Attacks
Having internet connectivity presents access points for attackers to breach an entry point and use it as a gateway to exploit devices on a network, especially if they have a weak or old password.

Mitigating Attacks

1. Consider using ISO 27000 Information Security Management Systems series of standards. Applicable to organisations of all sizes and in all sectors, this standard has been designed to assist companies in managing cyberattack risks and internal data security threats.
   https://www.iso.org/news/ref2266.html

2. Use ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection as a guidance document for defining and implementing controls for information security risk treatment in an information security management system (ISMS)
   https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

3. Conduct a risk assessment to identify areas of vulnerability that could potentially be exploited and uncover potential gaps and problem areas in your data security controls.

4. Establish network access controls and password policy to help mitigate the risk of insider threats. Assesses each user's access rights on an as-needed basis depending on job function to minimise the likelihood and impact of a deliberate attack or employee negligence.

5. Implement firewalls, malware and antivirus software as they offer an extra barrier to your network and devices.
   Firewalls provide a buffer between the outside world and your network to give more significant control over incoming and outgoing traffic.
   Malware and antivirus software searches your network and devices to identify any potentially malicious threats.
   Keep software updated with the latest patch release to stay ahead of attackers.

6. Continuously and proactively monitor network traffic to remain ahead of cybercriminals. There are some tools that will enable you to view your IT network at any point in time to actively identify new threats and determine the optimal path to remediation.

7. The most critical element in mitigating cyber risk in your organisations, is to educate and ensure everyone understands what they're responsible for to prevent a cyberattack or data breach.
   An incident response plan should detail where threats can come from and how employees can report a potential threat such as a phishing email. This will ensure everyone does the right thing to proactively prepare to move quickly and efficiently to remediate any issues.
   Staff should have regular training, and the incident response plan should be kept up to date to protect against any new threats.

Conclusion

Most perpetrators want to steal money by gaining access to credit card information, personal data, usernames and passwords.
Other cybercriminals use corporate espionage by stealing valuable sensitive data, if breached would damage a business' reputation or cause harm if information about new products, or services were leaked to a competitor.

The increasing cyber security risks facing your organisation presents many challenges including:

Bring your own device (BYOD) staff using their own devices means you have little or no control over how they are configured, potentially putting your network at risk each time the device connects to it.
The Coronavirus pandemic lockdowns may have resulted in employees permanently moved to remote working giving you less control over their behaviour and device security.

Doing nothing is no longer an option and organisations must protect their business and reputation by establishing at minimum basic cyber defence security controls and processes.
Preventing, detecting, or disrupting an attack at the earliest opportunity limits the impact to day-to-day business

Image Credits

Introduction to Cybersecurity – Gorodenkoff
Script Kiddies - Sora Shimazaki
Types of Cybercriminals - Victoria Borodinova
Scammers - Cyan

Disclaimer

Due to Cyber threats frequently changing, and Artificial Intelligence (AI) being a major contributor to the advancement of cyber security, in the identification of malicious behaviour from hackers by using machine learning to improve threat detection.

P4P Compliance Management Limited work very hard to provide up-to-date accurate information through thorough research at the time of publishing; however, some information may understandably be less accurate as time passes. We make no representations or warranties of any kind (expressed or implied) about the completeness, accuracy, reliability, suitability or availability of any information, products, services, or related graphics contained in this article.

All images used in this article are purchased, free stock, or CC0 licenced and accredited to the artist where possible.