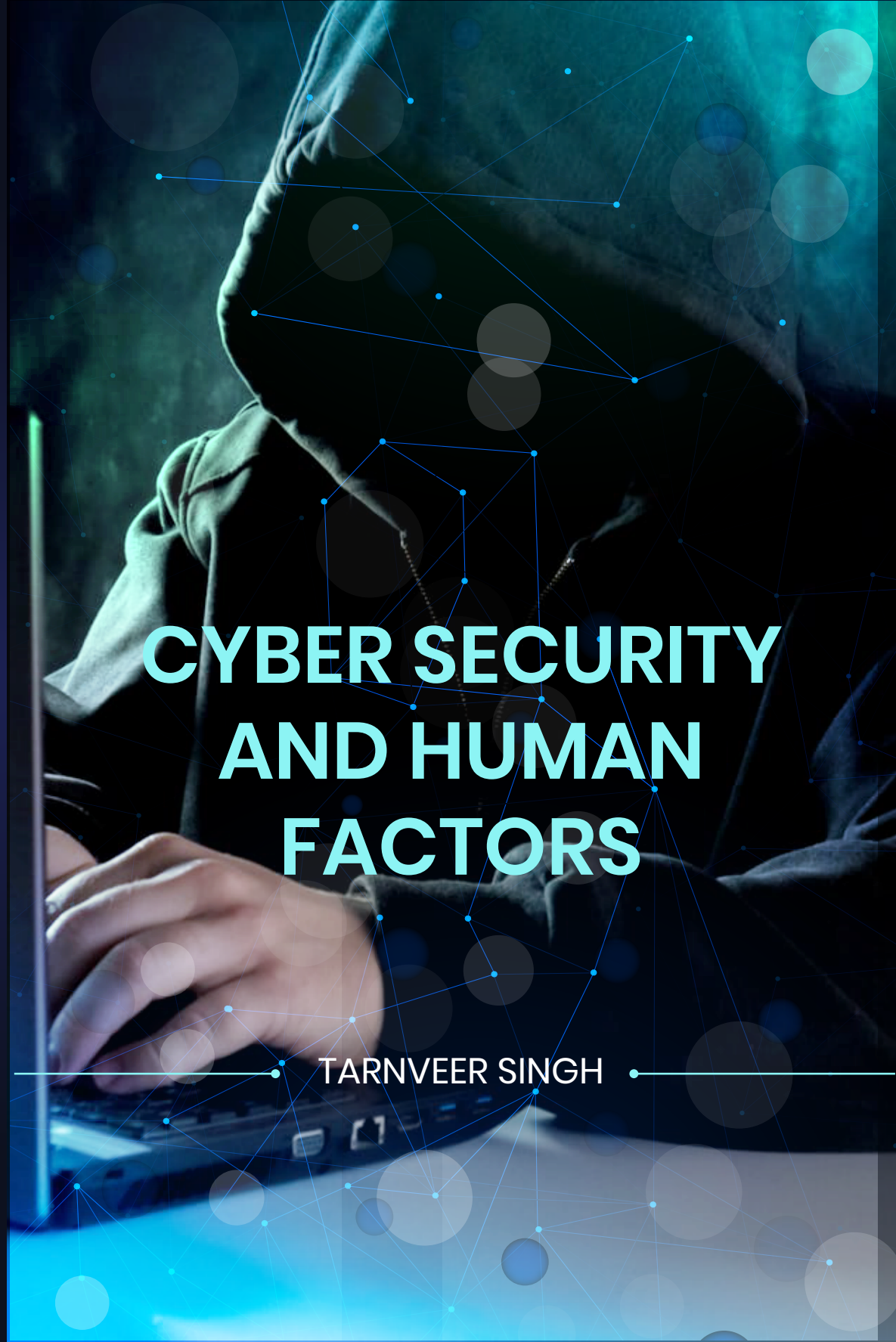

CYBER SECURITY AND HUMAN FACTORS

TARNVEER SINGH

CYBER SECURITY AND HUMAN FACTORS

KEEPING INFORMATION SAFE

TARNVEER SINGH

This book is dedicated to my seven year old daughter whose love and curiosity inspired me to write this book. The next generation deserves better and this book intends to spark discussion on how we can improve cyber security and safety.

CONTENTS

SECTION 1:

CYBERSECURITY: GETTING THE FUNDAMENTALS RIGHT

Introduction

In recent years, it has been clear that many services and applications are utterly unsecured, and that they can often leak our personal information, location, and credentials, whether by accident or deliberately.

This has caused a paradigm shift in the crime. Bank robbers used to solely rob banks because that's where the money was. While this may still be true, stealing money from a computer on the other side of the world is far less perilous than breaking into a bank or holding up employees with a shotgun. It can also be a lot more profitable, as we'll learn later in this book.

We are concerned about our privacy, yet we are willing to disclose our home address, email address, and credit card information to a company we have never heard of in exchange for a discount. We're lucky most of the time: the company turns out to be legitimate, and we get exactly what we paid for. However, we may not always be so fortunate - the offer may be a ruse, or the company's records may have been stolen, including the personal information we have provided, and now an unknown third party has it, which they can exploit, mistreat, or sell.

We feel threatened when we hear about new legislation that appears to give the police and security services an unrestricted right to snoop into our private lives. But we also feel encouraged when we hear that the security services have used the same legislation to intercept terrorist communications and prevent an attack. We understand that such surveillance is necessary, but we don't want it to apply to us because we haven't done anything illegal.

Cybercrime is becoming significantly more common than traditional burglary for the majority of individuals. When we buy things online, especially software for our smartphones and computers, we have to agree the seller's terms and conditions, but do we ever read them before clicking 'Agree'?

We expect that terms and conditions will be fair and meet with legal and reasonable trade standards, but they are frequently so long and written in legalese that we quickly lose interest in reading them. Of course, if you don't click 'Agree,' you won't be able to utilise the facility or software or at least only a limited version of it. We download 'apps' for our smartphones and tablet computers to make our lives easier, but many of them use the device's location whether we want them to or not, and this information can be collected, aggregated, and sold to others.

So, when things go wrong, we must bear at least some of the guilt - after all, we have given away information that may be used to identify us, as well as the opportunity for someone else to profit at our expense, whether intentionally or innocently.

The issue, however, is much larger than our individual shortcomings. Attackers will try to obtain information about us through using insecure applications and web-based services, and in this situation, the organisation that hosts the service and stores the information, rather than the consumer, is responsible.

While most organisations that are hacked remedy the problem (closing the stable door after the horse has bolted), some amend their terms and conditions to put the onus back on the customer in the event that their website has vulnerabilities.

Failure to secure our computers, smartphones, and tablets, as well as willingly handing up our credentials to strangers, is the digital equivalent of leaving the house unlocked and the keys in the car on the driveway when we leave on vacation.

There are so many data sources that listing them all would be impossible, but let's look at a few that might have an impact on our daily life in the context of cyber security. Our mobile phones capture call data records that detail who we phoned, when, from where, and for how long. Facebook, Twitter, and LinkedIn are just a few of the social media sites that gather text and photos. Location data from mobile phones and images we've shared can be recovered using the Global Positioning System (GPS). Data is collected through the usage of travel cards on buses and trains. Running shoes and body sensors provide data for fitness tracking. Data from congestion charge cameras, as well as data from number plate recognition, is collected. Credit and debit card transactions reveal a wealth of information about our personal habits. Personal information about us is contained in PayPal transactions and withdrawals from automated teller machines (ATMs). Passenger name records and loyalty cards on airlines contribute to data collection on our vacation habits, as well as information about us and our location. Because company ID cards were utilised for physical access control, data about us personally and our location was acquired throughout the working day. Our internet browsing history is connected to the MAC addresses and IP addresses of our computer devices. Bluetooth and wireless network (Wi-Fi) identifiers can be used to identify devices in a variety of ways. Passport scanners collect very personal data. Store loyalty cards allow us to track our purchasing patterns and see exactly what we buy on a regular basis. Access to our accounts and a plethora of sensitive information on us and our employers is controlled by user identifying names and passwords.

We could go on and on but consider this: if someone had access to all or even a significant portion of this data, they would know a lot about you, your movements, your business and personal relationships, your spending habits, your religion, sexual orientation and/or gender, political views, and your general health.

They might also expand their knowledge base by comparing some of your data to that of others, such as your Facebook acquaintances. This information is valuable not only to you, but also to others who might want to exploit it for lawful or illegal purposes. When we sign up for a "free" service, we are not getting anything for our money. We are exchanging some of our personal information for that service, and once we have handed it away, we no longer have control over it.

There are several basic words that should be grasped when discussing information security (including cyber security needs). The information security triangle — confidentiality, integrity, and availability – is a good place to start. However, there are two other terms that are currently considered to be equally important: authentication and non-repudiation.

Confidentiality refers to making sure that information is not revealed or made available to people who aren't supposed to have it. Loss of secrecy can be viewed as a goal in and of itself, such as the formula for a new drug, or as a means to an end, such as a password or PIN that grants access to a bank account. In either situation, a breach of confidentiality can have a significant impact on the individual or organisation that is the victim of a cyber-attack.

Integrity is concerned with the accuracy of data, regardless of how it is kept or communicated. Integrity entails ensuring that only authorised persons can produce, edit, or delete data, and it's strongly tied to confidentiality because it's usually those with unauthorised access to data who cause integrity problems.

Unauthorized changes to a student's grades from a 'fail' to a 'pass,' or unauthorised changes to a user's access level from 'guest' to 'administrator,' changing a criminal sentence from a custodial sentence to a fine, altering a mortgage applicant's credit rating, or removing details of previous illness from someone's medical records are all examples of integrity failures.

Availability refers to the ability of systems and the information stored on them to be accessed when and by whatever means are agreed upon. Customers of a bank, for example, would fairly expect to be able to access their accounts at any time of day or night, whether through online or telephone banking. Failures of availability almost always cause inconvenience, such as banking system failures which leave customers without access to their accounts and prevent inter-bank transfers. However, in extreme cases such as access to a hospital database containing details of an unconscious patient's allergies, they can be lifesaving.

Although the first three characteristics (availability, integrity, and confidentiality) have long been considered the "triad" of information security, the two next factors (authentication and non-repudiation) are also strong competitors.

Authentication is critical because it allows a system to confidently identify users. The traditional username and password have long been thought to be insufficient for making a positive identification, so additional methods have been introduced, one of which is 'two-factor' authentication, in which the traditional username and password (something you know) are supplemented by another form of identification, such as a token or smartphone app that generates a time-dependent one-time random number (something you have), or a biometric factor such as a fingerprint or iris scan (something you are).

Non-repudiation is equally important. In the event of a breach of confidentiality, integrity, or availability, even if someone has approved access to a system or information, they can deny taking the action that caused the problem. Non-repudiation is the process of ensuring that properly authenticated users cannot deny performing a specific action. This generally means that a detailed audit record of every activity taken by the user is retained.

Security is a phrase that encompasses both confidentiality and integrity, as well as availability to a lesser extent. It merely means that anything is safe from illegal access or harm, but the concept doesn't go any further.

When we, or our property, is protected from unwelcome intrusion, whether through the use of physical locks or a fully electronic device that prevents admission to those who do not have the correct keys, we feel safe. Security isn't just a technical or physical condition; it's also an emotional state of mind.

Privacy on the other hand, has a slightly different connotation. While the same principles apply as with security, privacy takes a more personal approach in that the subject matter, rather than being broad in reach, is much more personal to us. For example, someone living under a repressive government may regard the privacy of their political ideas greatly.

On the surface, security and privacy appear to be very similar, and in some cases, they are. However, there is a conflict between the two: for example, we rely on the government to keep us safe, both individually and as a nation, but we may believe that in order to do so, they have intruded on our privacy by intercepting our internet transactions and emails. It is possible that security will come at a cost.

Trust is the firm belief in the reliability, truth or ability of someone or something. It's very easy to lose trust, and it's very impossible to regain it. We put our faith in people, organisations, and systems without always thinking about or considering the implications. When trust is destroyed, the party responsible may suffer irreparable reputational or financial harm, such as when an online trader 'loses' our credit card information along with the information of thousands of other consumers. On rare occasions, however, the stock price returns to normal or near-normal levels.

Big data and data mining encompasses not just vast amounts of data, but also many data sources and their consolidation, as well as the skill and desire to sift through records and identify patterns, thereby transforming data into knowledge. For example, consider a large ecommerce website: its databases may contain the registration and payment information for millions of customers; tens of thousands of items; the combination of which consumers have purchased which things; and when, when, how much they paid, and how they paid. The ecommerce website's capacity to make solid business decisions with that data is enormous, but only that skill will decide its ultimate value to both the ecommerce website and the consumer.

The process of acquiring massive data is referred to as data aggregation. Some large data (like in the example above) comes from a single source, while other applications will necessitate the inclusion of multiple data sets. These can be obtained directly by the organisation that requires the data, or they can be brought in from outside if they are not available within the organisation. Data aggregation may be a very powerful method for integrating seemingly unrelated data sets into one that can be utilised to create a complete profile of a subject if done correctly. Data aggregation, on the other hand, is much more than a way of getting massive data. Combining poor classification data sources, for example, can result in a gold mine of personally identifiable information, posing a whole new set of security concerns (PII).

Cyber security is intertwined with a number of different types of security. It overlaps with information security, which is concerned with the protection of confidentiality, integrity, and availability of information in all areas, not only cyberspace. It also has some overlap with application security, which is focused with introducing controls and measurements to an organization's applications, whether software, hardware, or data. It is similar to network security, which is concerned with assuring the security of an organization's networks, both within and between organisations, as well as between the organisation and its users. Server operating systems (OS) and, increasingly, the virtualization layer and accompanying management tools are all part of network security. Furthermore, cybersecurity intersects with Internet security, which is concerned with preserving an organization's internet-based services' availability and reliability, as well as protecting individual users at work and at home. It also overlaps with critical information infrastructure protection, which includes the cyber security aspects of critical information infrastructure (CII) elements of a country.

What Impact Could Cyber Threats Have?

Cyber impacts or consequences are the result of an unintended incident, such as when a threat exploits a vulnerability. Impacts come in a variety of shapes and sizes, but they all necessitate some sort of decision. Some affects can be accepted because they are minor, but many cannot and must be mitigated or eliminated through some type of countermeasure, control, or treatment. Many of the consequences will be felt on a personal or individual basis, while others will have a far broader impact on businesses.

Individuals in the home or in small businesses, as well as those working in major corporations, are affected by personal impacts. The loss or disclosure of personal information is one of the most concerning consequences for individuals. This might be nearly anything about our personal or professional lives that we'd rather keep secret, but which, for whatever reason, would become awkward or embarrassing if made public. It's remarkable how much information you can gather about someone without ever having heard of them or knowing that they are aware of the situation. There are a lot of people with the same name, and they all seem to have the same email address. Many of us get emails addressed to others on a regular basis. It is easy to build up a blurry picture of them over time, completely accidentally. We know their names, their occupations, where they reside (approximately and in a few cases, exactly), their interests, and some of their buying patterns. I'm sure I could learn a lot more if I set my mind to it, but the more essential point is that they are either completely unaware of this or absolutely indifferent that much of their personal information has wound up in the hands of someone for whom it was never meant.This is due to one simple fact: they wrote their email address wrong, or the person who sent them an email did. We gladly sign up for social media sites and provide information about ourselves. Facebook, Twitter, and LinkedIn are just three examples of social media platforms where a wealth of information about us may be uncovered, including our prior schooling, university experience, work history, interests and hobbies, family life, and much more. Individuals aren't the only ones who can generate issues for themselves. Consider the instance of a CEO who was meeting with the CEO of another company on a regular basis in order to discuss a merger. His teenage daughter shared a photo of the place they visited, along with a message about her father being in a meeting at a particular company, on one occasion when he had his family with him. Someone who followed her on social media put two and two together and made a few phone calls, resulting in the fact that a highly sensitive debate became public information, impacting the firms' share prices and effectively sabotaging the project.

Credentials of individuals are major business. Bank and credit card account information, usernames, email addresses, passwords, and other personal information are bought and sold on the internet for surprisingly low prices. An attacker who can obtain these in quantity can profit from the information in a number of ways, including using the credentials himself to carry out attacks against the individuals in question, or selling them in bulk to others who are better suited to carry out the assaults. Depending on the sort of credentials revealed, the consequences on the individual can be significant. If the victim is fortunate, they may be able to detect the attack early on and only lose a modest amount of money. It can be considerably more catastrophic if they are unfortunate.

Money is a primary motive for cyber-attackers, thus if the opportunity arises, they will strive to steal as much as they can. In some cases, where the individual can demonstrate that they have done their due diligence and protected their computer and bank cards as best they can, the finance organisation will accept responsibility for the losses; however, where individuals have been careless or negligent, they risk losing significant sums of money. If, for example, a loss empties one's bank account right before to a direct debit being taken for a mortgage payment, and this is then indicated against the individual's credit rating, the individual's financial standing or credit worthiness may be impacted.

Personal reputations can readily be ruined by cyber-attacks. Consider someone whose email account has been hacked or whose account username has been used by an attacker. It is relatively easy to send out harmful emails that might ruin their reputation overnight. More often than not, especially if the recipients know the person well, they accept that the account has been abused, but the consequences of receiving hostile communications from someone you don't know can be far more serious. Reputation and trust go hand in hand. People with a good reputation are more trustworthy, and vice versa, and losing trust in someone means that their word is no longer trustworthy.

Theft of intellectual property is closely tied to the theft of money, because even if no money is taken, the IP owner's ability to generate money through sales is taken away. An attacker stealing the original material and claiming it as their own is a secondary and far more serious loss of IP, putting the original IP owner at a severe disadvantage.

Identity theft is widespread among persons who are targeted by organised groups that use that person's email address to send hate mail to everyone on their contact list, steal money from their bank account, rack up credit card bills, and nearly destroy their personal and professional lives. While the culprits could be identified, they would never be prosecuted because they would be beyond the security services' authority.

Because an attacker may betray their identity if they carry out too many actions using the stolen identity, identity theft is frequently linked to cyber theft, but in the event of a quick 'smash and grab,' the attacker can discard the identity as soon as they have the money.

Organisational impacts Include many of the above. The overall impacts, however, could be substantially bigger due to the scale of organisations, both in terms of the number of people involved and the amount of money involved. These might easily include a company's partial or complete demise, as well as significant job losses.

When a cyber-attack is successful, the organization's brand and reputation are usually harmed, especially if it becomes evident that the organisation did not take any precautions either to prevent the assault from occurring in the first place or to successfully deal with it once it has occurred. It's sometimes because one or both of these have resulted in the loss of intellectual property or customer data. Customers may lose trust in organisations that have suffered such an impact and opt not to do business with them in the future.

The financial impacts on a company's revenue streams might be disastrous. Customers will be unable to place orders as a result of cyber-attacks, and an organisation will be unable to trade online. This will not only result in immediate revenue loss, but it will also frequently result in downstream losses when clients move their company elsewhere.

Following a successful cyber-attack that damages the company's brand, the stock price is likely to plummet. A decrease in share value is a common occurrence under normal conditions and would not be cause for alarm, but in these unique circumstances, it could take months or years for an organisation to recover its share price.

Furthermore, cyber-attacks might prevent an organisation from ordering items from suppliers, paying them for things already received, or paying employees' wages or salaries. Organizations can be penalised for mishandling client data in some instances, notably in highly regulated industries, especially if their acts violate data protection legislation. They may also incur further financial losses as a result of interest charges for late payments, particularly to Her Majesty's Revenue and Customs (HMRC) for late corporate tax payments.

In addition to any revenue losses, businesses will incur expenditures in repairing damage caused by a successful cyber-attack, which may entail the implementation of corrective information security policies. There's a chance that a company may be targeted by ransomware and will be forced to pay a ransom to get their data back. The alternative would be for the company to spend a lot of time and money trying to recover all of its compromised systems. The cost of such a recovery process could in some situations far outweigh the ransom demanded.

When an organization's operational systems, such as development systems, production control systems, stock control systems, and the like, are harmed by a cyber-attack, operational failures can ensue. The consequences could be disastrous, as the organisation may be unable to function for the duration of the situation.

Most, if not all, of these failures will undoubtedly have financial consequences, since the organization's ability to offer products or services to its consumers will result in revenue loss, as well as possible brand and reputation harm.

The failure of a software upgrade at the Royal Bank of Scotland a few years ago resulted in 6.5 million clients being unable to access their online accounts, receive incoming payments, or make transfers to other RBS or other bank accounts. Various regulatory organisations fined the bank a total of £56 million. While this isn't a specific cyber security event, it does show what can happen when system upgrades aren't thoroughly verified before being deployed.

Employees who are forced to be laid off as a result of financial losses or operational failures, or who choose to quit because they have lost faith in the organization's capacity to appropriately plan for and respond to cyber security disruptions, can have a significant influence on people. These personnel losses result in a significant loss of expertise.

Cyber Crime

Cybercrime can be avoided with the effective use of information security. Cybercrime definitions are riddled with flaws. Many cybercrimes look like 'normal' crimes, but they always have a cyber component to them - either as a means to an end, including cyber systems or networks, or as both a means and a target, involving cyber systems or networks. Anyone can be a victim of cybercrime, whether or not they are online. Even if you have never used a computer, a criminal can spend your money once they get your bank or credit card information.

Cybercrime can encompass but in no way restricted to:

- **Cyber-trespass:** Like its pre-digital cousin, this category combines together cyber-offenses that include 'crossing or violating borders,' however these are digital rather than physical barriers. For example, the cyber-trespass category could include offences like hacking or unauthorised data access.

- **Cyber-deception and theft :** This category includes crimes like online fraud and IP theft, which are typically addressed separately.

- **Cyber-porn and obscenity:** In addition to the well-known range of child pornography-related offences, Wall's category included other sorts of online sexual behaviours that are generally frowned upon but not criminalised, such as the distribution of pornography.

- **Cyber-violence.** This encompasses the types of emotional violence that can be perpetrated online, such as bullying and harassment. However, there is also mention of more extreme acts, such as cyberterrorism.

Illegal interception, data interference, system interference, and device misuse are all examples of crimes against the confidentiality, integrity, and availability of computer data and systems. Forgery, fraud, and other computer-related offences are examples. Child pornography and terrorist materials are two examples of content-related offences. There are copyright and associated rights-related offences. There are additional secondary liabilities, such as unauthorised access.

Financial theft, on the other hand, is the most common sort of cybercrime. Unlike a traditional bank robbery, when physical currency is stolen, this form of crime poses little or no risk to the criminal, as there are no firearms, masks, or getaway cars, and it can result in a far larger payoff.

One disadvantage of cyber-based financial theft is that there may be an audit trail identifying where the money came from and where it was transferred to. Money laundering and utilising middlemen to distance themselves from the criminal conduct have been used by cyber criminals to remedy this flaw in their scheme.

Cyber criminals are increasingly less interested in obtaining individual personal details in order to commit crimes, not that we should be complacent about this, but instead are looking for details of thousands or millions of individuals' personal details in order to maximise their return on investment, because each piece of information has a value.

They frequently accomplish this by selling the information to larger criminal gangs, whose resources enable them to utilise the information in large-scale spam campaigns, such as those purporting to sell high-end watches and mobile phones.

Alternatively, criminal gangs target specific groups of people by offering non-existent vehicles for sale on legal websites. After agreeing to purchase the vehicle via email with the fraudsters, buyers receive an email pretending to be from Amazon indicating that their money would be kept in an escrow account until the buyer confirms that they agree with the arrangement, thereby providing 'buyer protection.' Of course, after the buyer has deposited the funds to the 'escrow account,' the transaction is complete, and the vehicle is no longer visible.

The term 'hacker' originally referred to someone who was curious about how things functioned, dismantled them to learn more about them, and then reassembled them in a way that improved their performance. A hacker was eventually defined as someone who built software that performed a beneficial activity in a graceful manner. A piece of code that was condensed to run in a relatively small memory space was deemed a "wonderful hack" when computer memory was an extremely expensive commodity.

Some of the greatest inventions have come from this benign activity, but unfortunately, the term 'hacking' has been tarnished by the media in recent years, referring to those with less honourable intentions who break into other people's computers for fun, revenge, or to make a statement of some kind – often on political, ethical, or environmental issues, and some hackers will simply deface a website (usually its 'landing' page) in order to make a statement of some kind – often

Some hackers merely break into a system "because it exists" and "because they can." This serves no use other than to show their friends how brilliant they are and how vulnerable the target's security is. This intrusion, known as 'planting the flag,' is intended to demonstrate their achievement and, hopefully, garner them the respect of their colleagues.

This type of hacking can be quite benign at times, yet it can result in the defacement of internet pages. This type of hacker is often referred to as a "script kiddie," who takes advantage of software and techniques they've discovered in the darkest corners of the internet, and while they may mean no harm, serious damage can easily occur due to their limited knowledge and ability to use the software and tools. Script kids, on the other hand, can evolve into full-fledged cyber criminals if they are encouraged and given the opportunity to do so, and this can result in significant damage.
Many organisations affected by this type of hacking admit to being careless with their cyber security and respond by tightening their security practises, while others, as in the case of George McKinnon, who was accused of hacking into NASA and US military computers, may press for arrest, prosecution, and even deportation.

Exploitation elevates intrusion to a whole new level. A hacker who exploits a system they've broken into may exfiltrate, erase, or distort data, which can have disastrous consequences not only for the target organisation, but also for its customers and system users.

Denial of service (DoS) attacks are commonly used to prohibit genuine users from accessing a company's website, while they can be used for other purposes. The reasons for this will vary – some will be used as a form of blackmail (pay us money, and we'll stop); others will be motivated by political or other activism (commonly referred to as hacktivism) and will aim to cause financial loss and/ or public embarrassment; and still others will be in retaliation for some real or perceived action.

Some DoS attacks are aimed to crash a website by overloading it to the point where it can no longer function, while others merely block lawful access, preventing the supporting apps from receiving and processing service requests. In either case, the website's response will be significantly slowed and, in most cases, totally halted. DoS attacks can also be directed at an organization's email service, such as by a disgruntled employee, causing the Exchange server to become overburdened and stop handling valid email traffic.

The distributed (DDoS) attacks are the most common types of DoS attacks nowadays, in which numerous computers cooperate together to overload the target website. Because very few stand-alone systems are capable of successful attacks against very big websites, attackers usually employ botnets to assemble sufficient capability.

Copyright infringement is a big business, although it usually only pays out in the form of 'free' items for the recipient. Music, films, books, photos, and computer software are all examples of copyright infringement. While the copyright holder usually retains ownership of the item, illicit copies are made, depriving the owner of the profit they may have had from it.

Copyrighted material is frequently transmitted through file-sharing websites like The Pirate Bay, which use so-called "torrent" files to direct consumers back to the specific file or files to be downloaded. The downloaded material is shared amongst users as more people join the sharing process, and dissemination is peer-to-peer.

Because many copies were produced in such a short period of time, it is also impossible to identify the person who originally hosted the information. While torrenting files is not illegal, the content may be, especially if it is protected by copyright and the owner has not consented to it being shared in this manner. The annual losses to numerous industries are estimated to be in the billions of dollars.

While intellectual property theft is comparable in many ways, the sale or dissemination of the stolen property is usually not. Unlike copyright infringement, which allows a large audience to benefit from free software, music, or video material, IP theft is more commonly done to order for one or a few select customers, and rarely becomes widely spread. Previously, this would have been referred regarded as 'industrial espionage.'

The financial loss to the owner, on the other hand, can be enormous, especially when a pharmaceutical company develops a ground-breaking treatment only to lose its formula to a competitor who can then sell it for less than the cost of production, packaging, marketing, and distribution.

While the employment of so-called dark patterns isn't illegal, it does tend to blur the line between fairness and dishonesty. When you visit a website, you may discover that, due to imprecise writing on web pages, you have consented to download software or accepted an offer that you did not mean to accept. Web page designers often purposefully place selection boxes in strange places or make the options difficult so that you are compelled to make their choice rather than your own.

There are entire industries dedicated to determining the shapes, sizes, and colours of buttons, click boxes, and text that users are most likely to click on – and those that they are least likely to click on – while visiting a website. The data is sold to companies that are creating new websites or updating existing ones, with the goal of enticing consumers to choose the company's option rather than their own.

In extreme circumstances, products you didn't request may be added to your online shopping cart, and if you're not careful, you can end up buying something you don't want as well as the items you want.

Dark patterning is the act of making web sites perplexing, and the techniques are incredibly subtle, based on established features of human behaviour. If you are trying to book a flight, for example, you may notice that the airline or travel agency offers to sell you travel insurance, and unless you choose to opt out rather than in, you may discover that you have purchased it and may have problems getting a refund.

These black patterns aren't strictly forbidden, but they represent sharp practise in the imaginations of many individuals. Although pressure groups are forming to combat this by establishing a code of conduct for web developers, it is possible that only legislation will fully resolve the issue, as the offending organisations' sales and marketing policies are likely to drive the practise for the foreseeable future, especially where it increases revenue.

Cyber Safety

The act of harassing or bullying an individual or group of people via cyber-based technologies such as social media, text messaging, and the like is known as cyber harassment or cyberbullying. I chose to separate this from cybercrime since some components of cyberbullying are not technically criminal or civil offences, yet they are a huge problem in today's society. Some jurisdictions, however, have enacted legislation that expands the definition of harassment to include internet harassment. The distinction between online harassment and cyber bullying is that with internet harassment, anyone or any organisation can be a victim, whereas with cyber bullying, the victims are primarily children.

Cyber harassment or bullying can start in the same way that traditional harassment or bullying does, with a nasty comment about another person that offends them. The bully (who may or may not be a control freak) seizes on this effect and exploits it again and again, often urging others to join in. The consequences can be severe, and some people who have been harassed or bullied for a long time have been forced to commit suicide. Cyber bullying or harassment is just as aggressive and deadly, and it can come in a variety of forms.

Cybercriminologists have spent a lot of time looking for online behaviours that influence the chance of committing a crime or being a victim. While some of these criteria have remained important as technology has progressed, others have become less so in terms of identifying cybervictimization. Before getting into specific behaviours, it's important emphasising that many academics continue to emphasise the link between growing online presence and criminality simply as a matter of opportunity. To put it another way, as one's online profile grows, so does the chance of being a victim of or perpetrator of cyberbullying. Scholars have discovered numerous harmful online behaviours that influence the probability of cyberbullying perpetration and/or victimisation. Given the nature of cybercrime, the most problematic activities reported across the literature are those that place persons in close contact to others, which makes intuitive sense. Many studies have discovered that children who use chatrooms, instant messaging, and social media sites are more likely to be victims of and perpetrators of cyberbullying. Furthermore, numerous studies have shown that those who participate in risky behaviour that displays vulnerability are more likely to be subjected to cyberbullying. Bypassing security systems, uploading risqué photographs, or victimising others, for example, raises the danger of being subjected to cyberbullying.

Given the well-documented dangers of social networking sites, researchers have concentrated their efforts on determining which behaviours on these platforms influence the likelihood of perpetrating or being the victim of cyberbullying. Although this field of study is still in its early stages, scientists have discovered that having a large number of friends, engaging in negative content (directly or through friends), making status updates, and using private messaging all raise the likelihood of being subjected to cyberbullying. Despite the importance of this online behaviour, researchers have focused on determining whether particular offline behaviours influence the probability of experiencing or perpetrating cyberbullying. Cyberbullies may, predictably, exhibit clinically abnormal levels of disobedience and use addictive substances. Cybervictims, on the other hand, may be more likely to suffer from despair and other harmful repercussions.

Cyber harassment is intended to alert the victim to the possibility of something specific happening to them. Threats can be made by people who are known to the victim or by people who are unknown to the victim, and targets can be broadened to include organisations that the person issuing the threats believes have wronged them or someone else.

Sending threatening and unwanted communications over omnipresent platforms (i.e., email, instant messaging, social media), as well as leveraging publicly available online information for criminal objectives, all fall under the definition of cyber stalking. Cyber stalkers operate in two modes. First, they can watch their victim's movements and activities invisibly, without alerting them to the fact that they are being followed. Second, they can still track their victim's movements and activities, but this time more openly, with the victim being aware that they are being followed, but usually unaware of the stalker's identity. The victim may be someone the stalker is familiar with, such as a relative, former partner, or neighbour; nevertheless, the victim may be someone the stalker is unfamiliar with, such as a celebrity, an organization's CEO, or a politician. Cyber stalking's main goal is usually to create distress to the person who is the target, and it is commonly successful. In certain cases, cyber stalking involves instilling fear in the victim by informing them that the stalker is watching them, but this is usually where it ends.

Cyber trolling is a type of verbal abuse intended to intimidate or offend the target. Cyber trolls engage in confrontational or unpleasant online behaviour and, unlike cyber stalkers, make little effort to conceal their identity. Online trolling is also distinct from cyber bullying or harassment in that it is done openly, maybe in the hopes of gaining support for the cyber troll's point of view and is intended to cause the victim anguish. Cyber trolling also varies from free and intelligent debate in that it does not allow or encourage a rational exchange of ideas, instead focusing solely on the cyber troll's negative, often strongly voiced, and generally irrational viewpoints.

Cyber trolls will frequently post inflammatorily comments on social media or online discussion forums in order to elicit a reaction or response from the victim, which will invariably provide the troll with more opportunities to post comments, and this can quickly escalate into a full-fledged online brawl. According to conventional opinion, the best method to deal with cyber trolls is to ignore their comments, as their actions will quickly fade if there is no reaction, response, or interaction. Alternatively, offending people can be disabled on many discussion boards, preventing victims of trolling from seeing their comments. Trolls can be reported to the forum moderator, and their accounts may be terminated as a result.

Cyber warfare is the process by which one nation state or politically motivated group attacks another's critical infrastructure (CI), political process, or even offensive or defensive military capacity. Warfare was, until recently, a rather simple process. One country state picked a conflict with another, and their two sets of armed forces went at it until one nation state capitulated and the war was done. Only when more country states joined in on either side did things get really difficult, but the end conclusion was typically the same. Because both 'sides' are usually evenly matched, this type of warfare is commonly referred to as symmetric warfare.

The growth of terrorism, on the other hand, blurred the lines. A militant group might declare war on a number of countries, often without regard for whether or not those countries shared the same religious or ideological beliefs. Because terrorist groups rarely have the same purchasing power as nation states, their weapons are frequently home-made such as improvised explosive devices (IEDs), for example, but because they can be used in unconventional ways – not just in battle – they are frequently deployed as roadside bombs or detonated by suicide bombers. Asymmetric warfare is named by the fact that one side may have a tiny number of soldiers compared to the other yet can still deliver devastating effects. A cyber-attack or cyber invasion by one nation state against another, on the other hand, does not necessarily imply that they are at war, and the attack could merely be viewed as an act of aggression rather than a formal declaration of war.

Because technology can be deployed by one nation state against another, or by small groups – even individuals – against a much bigger foe, cyber warfare employs both symmetric and asymmetric means. Unless the other side can find the attacker and instruct a drone to deliver lethal ordnance, cyber warfare can be performed just as readily from an armchair, a stool in a cybercafé, or an office chair in a government building, and carries few of the perils of traditional combat. If they work for the government or military, or if they are a highly skilled and experienced individual, a 'cyber warrior' can walk home safe in the knowledge that they are unlikely to be shot at after completing their daily or nightly shift, despite possibly causing their adversary significant cyber havoc.

The capacity to gather secret information without the owner's permission or knowledge is referred to as espionage. Governments often conduct surveillance on one another. They've been doing it for centuries and will undoubtedly continue to do so in the future. Sometimes espionage is about discovering what another country possesses – such as its nuclear missile capacity – while other times it is about discovering another government's objectives, which may be more difficult to detect but can be surmised given enough data.

Cyber espionage is no different, however unlike traditional espionage, which requires spies to put themselves in danger by working in enemy territory, cyber espionage may be carried out safely from the comfort of one's own office with no risk to the spy. If a field agent is apprehended and exposed as a spy for another country, the diplomatic fallout can last months or years. However, because nation-state cyber espionage departments take great pains to conceal their identities and frequently disguise attacks as coming from somewhere else, it is difficult, if not impossible, to prove who carried out an attack, and assumptions, even if correct, are insufficient evidence.

Surveillance differs from espionage in several ways, not in the way it is carried out, but in the goals and purposes it pursues. Surveillance focuses on keeping track of people's activities, communications, and contacts, and in terms of cyber warfare, it's more analogous to terrorist investigations. Because both security services and the military must work together to track down suspected terrorists, there is a particular overlap in the strategies utilised by the two. Surveillance has played a key role in identifying and locating individuals and groups with clear intentions to commit acts of terrorism, and while the details remain classified, the government has stated that careful surveillance has prevented a number of potentially lethal attacks, and they are using this argument to push for legislation that makes it easier for security services to monitor the activities of the general public.

Although governments and security services do not openly discuss this aspect of cyber warfare, infiltrating activist groups has proven to be one of the most effective (though risky) techniques of conventional surveillance, allowing operatives to identify potential targets and their leaders.

In terms of objectives, cyber infiltration is no different, and agents must be able to infiltrate online groups just as readily, and because they are physically separated from the rest of the group, they are considerably less at danger if their activities are discovered, and they are 'outed.'

For its teams of saboteurs, cyber sabotage is far less dangerous. They will identify and monitor their target from afar, then carefully position their weapon, which will subsequently destroy the enemy's infrastructure, using one of the attack methods we've already discussed. It has been demonstrated that sabotage of key

infrastructure parts is conceivable. In 2007, the Idaho National Laboratory in the United States conducted a test in which it opened and reopened the circuit breakers connecting a 50 MW generator to the grid out of synchronisation, causing the generator to shatter. On a broader scale, the impact on a major power plant capable of generating hundreds of megawatts of electricity might have a significant economic impact on the country.

Only in terms of magnitude does psychological cyber warfare differ from cyber harassment or bullying. Psychological cyber warfare is carried out by much larger groups, such as terrorist organisations and country states, whereas cyber bullies are usually individuals or small groups. Psychological cyber warfare usually serves one of two purposes. First, it is employed by one organisation or government to demoralise the people of another country in order for them to withdraw their support for the present system. During World War II, both the Allies and the Axis forces used psychological warfare radio broadcasts to incite opposition to their respective regimes. Psychological cyber warfare merely shifts the medium from broadcast radio to the internet in this regard. The other goal is population enslavement and repression by the government – frequently an oppressive regime – which can utilise cyber tactics to prevent people from standing up to it and disseminate fear of the consequences of doing so. Not only do such regimes utilise the internet as a weapon in this way, but they also routinely restrict how the public uses the internet by blocking access to websites that do not favour or actively oppose the regime. Negative news reports about a dictatorship can be censored in the international press, and glowing portrayals of the regime's leadership and successes can be substituted — all while the people lacks the fundamental comforts enjoyed by less constrained cultures.

We are constantly under observation, whether we are aware of it or not. Cyber surveillance can be divided into two categories. The first that comes to mind is that of intrusive or invasive snooping, which is normally linked with security services monitoring, especially since the Snowden revelations. The second is the collecting and use of data about us by organisations with whom we engage on a regular basis, which appears to be far less intrusive on the surface.

The reason for targeted monitoring is because the subject has attracted the notice of the authorities, who are keenly interested in his or her behaviour. Normally (but not always), such persons are criminals or terrorists, and we are relieved to know that the proper police or security services are paying close attention to them. When we have the impression that we are being watched, we tend to take a different perspective, and it is here that we are aware of the problem that the police and security services face when they don't have a specific target in mind: they must collect far more data than they need, and then (in theory) discard the data that

isn't relevant or that they don't need to keep. Because the cost of storage media is continuing to decline, data collection and storage are becoming less expensive over time, and as a result, businesses will collect and store as much data as they can and preserve it until they figure out how to best use it.

In the wake of the Snowden revelations, blanket surveillance is becoming the standard. Security services on both sides of the Atlantic are listening in on phone calls, emails, internet searches, and transactions without necessarily having the legal authority to do so, which is concerning because we have no control over it. The word 'collect' has a different meaning for the National Security Agency (NSA). We would think of this as just data monitoring, interception, and storage, but the National Security Agency (NSA) views it to also involve data analysis.

How much personal information do you willingly give up when you look for anything on the internet? There's probably a lot more than you realise. Let's consider the case of Amazon for a moment. They retain a detailed record of everything you've purchased from them, so if you need something similar again, you can order it with a few clicks and without having to remember who supplied it.

They also keep track of all the items you've recently searched for. They are aware of your interests and wish to sell you more. Your search request is saved when you use an online search engine. The links that you click on after that are saved. Every website you visit on a frequent basis is automatically saved as a 'favourite' by the search engine.

Most Western countries enable the communications company supplying the service to keep records of any website and messaging service visited by their people from any device. The data is then accessible to government departments. Apart from the greater violation of privacy, one of the main worries is that all it takes is one bad actor to gain access to the entire database.

Not alone does search create a digital trace; every time you visit a website, a little file known as a 'cookie' might be left on your computer. Many cookies are required for you to be able to use the website - for example, when you shop online, the retailer needs to be able to link your shopping basket to your computer so that you can purchase exactly what you want. Other cookies are less useful to you, and they may keep track of which pages you've visited, whose flights you've looked at, or which cameras you've looked at. These may not appear to be particularly bad things, but the next time you visit an airline ticket website, it may just utilise the information that you've been there before to raise the ticket price or inform you that the cheaper flight is sold out and you must choose a more costly flight. Surveillance and subsequent manipulation are a very subtle sort of surveillance that we are typically unaware of.

Other cookies keep track of these details so that advertisers can place ads in prominent locations on the screen. If you use one of the major search engines or shopping websites to research a specific type of camera, you will almost probably see an offer from one of the photographic providers when you return to the site. This is harmless in and of itself, but keep in mind that the search engine or website may have saved every single item you've looked for. Advertisers can use this information to create a highly accurate picture of you as a person, and (in principle) offer highly relevant advertising to you. The advertiser will, of course, be advertising what they want to sell you, not necessarily what you want to buy.

The majority of websites do not allow you to disable cookies. They usually give you the option of clicking 'I understand' or something similar, 'Tell me more,' or simply ignoring the notice. Many websites employ an 'implied consent' approach, which means that if you ignore the cookie notification and continue to use the website, you have implicitly given your permission for cookies to be placed.

When you send or receive an email, your provider's server automatically saves a copy in case you need it later. Email analysis, whether obtained through interception or access to an ISP's servers, can provide a surveillance organisation with a wealth of information, as there may be a complete archive of all emails sent and received in the 'conversation,' and each email sent and received will contain details of the sender and recipients.

Email can be just as dangerous as cookies on a website. Unless you erase every duplicate of every email you've written or received, including those you've forwarded to others, the message will live on in some form someplace, and emails, like online searches, can tell a lot about you.

Unless all emails including personal information are encrypted, they can be read like a postcard, duplicated, printed, forwarded to others, and used in evidence against you if they contain something negative you have said or that implicates you in a crime. In the area of cyber surveillance, email may be a very effective tool, because not only can the content provide vital information to security services and law enforcement agencies, but the 'to' and 'from' sections in an email can also provide additional surveillance targets.

Email, far from being a blessing, may be a curse, and many of us would question how and why we have amassed so much rubbish in our inboxes. Receiving spam via email might potentially invite cyber-attacks.

Many people have abandoned their traditional mobile phones. The quantity of data that can be taken from you thanks to smartphones is mind-boggling. The phrase "smartphone" is most likely an oxymoron. The device is actually a small computer that runs applications, takes photos, and also makes and receives phone calls and

text messages, so it's not all that different from your laptop in that regard – just smaller and often no less powerful. Unless you turn off your phone, your network operator always has a rough idea of where you are and can route calls and texts to you. Unless you've gone into your smartphone's security settings, you'll almost certainly be recording your GPS coordinates, which will pinpoint your whereabouts to within a metre or two.

Every app on your smartphone that need your location to function can now track your movements. If you're using a mapping programme, this is ok, but if you're just playing a game, it's not. Of course, the app developer isn't interested in your location, but they might be selling your information, along with hundreds of others, to a third party.

Have you ever used your smartphone to capture a picture? The location was saved in the exif data, which is the metadata of a photograph. That exif data became available when you uploaded that photograph to the internet. The exif data will also include information on the date and location of the photograph, as well as the serial numbers of the camera and lens you used.

Individuals can be identified in real time using a contemporary camera or smartphone, or from a previously taken snapshot using facial recognition. The image is compared to others in a central database, and complex algorithms are employed to match features like the eyes, lips, and head shape, among others. Once a match has been made in this manner, more information on the person can be obtained, either from the same database or via a broader internet search. Although the police and security services must make extensive use of this in tracking down and monitoring suspected criminals and terrorists, we must face the fact that if someone's photograph is posted on the internet, they can be identified and possibly tracked regardless of whether or not they have committed a crime. However, if face recognition is used for authentication, it is easy to mislead the matching process by wearing a mask, therefore it should not be utilised alone. Consider someone who was photographed while participating in a nonviolent protest in a country where the government has complete control over its citizens. The demonstrator may then be visited by the secret police and disappear forever.

As we stated earlier in this book, terms and conditions can be a huge issue. We don't even look at them. Due to their length and confusing 'legalese' terminology, few people will have read them from beginning to end and will have simply clicked on the 'Accept' button, potentially relinquishing any control they may have had over their personal information. Of course, software sellers give us no choice - there is no discussion, and if we want the software, we must relinquish any rights we may have previously held. Furthermore, and maybe more concerning, by signing away our rights by accepting the terms and conditions, we may be exposing ourselves to surveillance, such as disclosing our location when using a smartphone.

When you initially use an app on your smartphone or tablet computer, you'll have to agree to the terms of service, which almost always include the ability for the app author's company to keep, use, and sell information about what you've done. Not only that, but because many of us don't turn off the GPS feature on our smartphones, the app may have the capacity to track your whereabouts and report it back to the provider — even when you aren't using it. Even if you read the terms and conditions when you first load a programme or make an online purchase, the seller may amend them at any time (their authority to do so without informing you may be embedded in the original terms and conditions), and you may never notice the changes.

Store loyalty programmes allow the store to keep track of everything we buy there, including how much we paid, where we bought it, and when we bought it. Store loyalty programmes are a fantastic invention. The deals that the store then offers us are usually good value for money, and they often help the store get rid of items that it wouldn't be able to sell otherwise. We may be eligible for a discount on certain items, free coffee and cake on our next visit, an invitation to a "special" pre-Christmas shopping event, or the opportunity to skip the line when a new product is released. Some stores now offer a smartphone app that allows you to access their website, your account, and a variety of other features. Have you ever received an email out of the blue from a company you'd never done business with before and wondered how you got it? It's very likely that you did so when you signed up for a loyalty programme. Many businesses use deceptive techniques to lead you to make the wrong decision when filling out such a form, and because you didn't read the terms and conditions, you may discover that you have agreed to the store selling your contact information to a third party. Of course, you can try to modify it, but it's usually too much trouble or the tools to do so are too tough to discover on the company's website, so you just accept it. Is this a problem with cyber security? Definitely, because a third party now has all of your information, as well as the information of the store that offered you the loyalty programme, and those details might end up anyplace if the third company's network is hacked.

Credit cards allow us to make impulsive purchases when we may not have enough dollars in our bank account; there is no financial charge if we pay off the outstanding balance on our credit cards each month; and they even operate as protection if something goes wrong when we make purchases. The same can be said about modern payment methods. mPay, ApplePay, AndroidPay, and travel money cards like Caxton all benefit both the provider and the consumer, but all come with the same level of risk. When you combine a credit or debit card with a reward programme, things start to look a lot better for the supplier. When you combine them with their smartphone app, which tracks your activities, you may find that the next time you go grocery shopping, you receive a text message when you pass a specific supermarket aisle offering you a special discount. Combine them even more where retailers provide the SIM card for your mobile phone (and

thus know your regular contacts and movements), and you may have agreed to allow the retailer to include the fact that their banking service is aware of all your current account financial transactions if you accepted the terms and conditions.

Travel cards allow you to load money onto the card and use it whenever you want – on the subway, buses, the river, and even some over-ground train services. Again, the card provider knows when you travelled, where you went, how long it took (except on buses, where you only use the card when you board and not when you leave), and where, how, and how frequently you topped up the card. All of this appears to be harmless because we benefit from much of the technology and services, but to return to one of the original points of this section, if the security services wanted to build a profile of you, it would be extremely easy to combine credit/debit card, store card, travel card, email messages, and internet searches with closed-circuit television (CCTV) images.

A data aggregator could create a detailed portrait of our daily lives. They'd know where we live, where we work, and possibly what kind of work we do; who our partners and friends are; when and where we shop; what and where we eat and drink; where we go on vacation; what music and films we enjoy; what newspapers and magazines we read; what television shows we watch; what kind of car we drive and where we go in it; and what hobbies we have. To put it another way, there's very little about our personal lives that is truly private any longer.

The sophistication of home entertainment systems has increased. Televisions can link to the internet not only to allow for the download of viewing material, but also to give manufacturers with data about viewing patterns. In theory, this type of remote monitoring should only be done with the viewer's explicit consent, but there have been instances where manufacturers have submitted watching data without the viewer's knowledge.

From a personal standpoint, we should always be concerned that our personal information is properly maintained and used. When our credit card company calls to question a transaction that appears to be outside of our normal spending pattern, we are grateful that they took the time to do so in order to keep us safe. As a result, we should be more cautious about the information we give out to others – information that could be abused or misused for their benefit at our expense; and reactively, if we suspect abuse or misuse of our information or credentials, we should change passwords and notify financial institutions right away. There are several reasons why we should be aware of cyber occurrences, plan to defend ourselves and our organisations from cyber-attacks and be ready to respond if they occur from a commercial standpoint. Managing risk, including the hazards of cyber-attacks, whether accidental or malicious, and whether as individuals or enterprises, is nothing short of best practise. Corporates (and board members) do have fiduciary responsibilities in this regard.

Customers have a right to expect businesses to protect their personal information when they give it to them for whatever reason, and they must have confidence that it will not be misused – in other words, strict respect to data protection laws. In highly regulated industries, businesses may be required to demonstrate compliance with national or EU law, international standards such as ISO/IEC 27001, and industry standards such as the Payment Card Industry Data Security Standard (PCIDSS), the US Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes– Oxley Act. As a means of gaining a competitive edge, businesses should be able to demonstrate excellent security practises. Some larger organisations may use ISO/IEC 27001 certification to demonstrate this, whilst smaller organisations that employ small-to-medium enterprises (SMEs) may use the UK government's Cyber Essentials and/or Cyber Essentials Plus programmes.

Rather than keeping our memories on paper, we now store them digitally. Letters, postcards, and photographs are all files on our computer, and when we compare information about us to footprints in the sand or an aircraft's vapour trail, the digital footprint pales in comparison. While physical footprints are washed away by the tide and vapour trails vanish, we continuously generate remnants that may last an eternity.

What Is Stopping Us?

Life is not as straightforward as we would like it to be, and there are a variety of impediments or barriers to meeting our privacy and security expectations, particularly for individuals, small businesses, and SMEs. Cyber security is sometimes regarded as a highly specialised subject, and many individuals and small businesses believe they lack the essential knowledge or skills to comprehend or carry out the work required to protect themselves against cyber-attack. Organizations of all sizes usually lack the personnel resources to devote to this type of job. The senior management team of the organisation may not fully comprehend the need of excellent cyber security and how it may benefit their business, as well as the fact that the data and hence the information held by the organisation belongs to them, not the IT department. When we look at the cyber security standards that have been developed, it appears that many of them are tailored toward larger organisations and multinationals. The Cyber Essentials scheme, on the other hand, addresses this for smaller businesses. Many SMEs outsource their IT, and many of the outsourced companies are likewise small businesses with limited cyber security expertise. When a company is able to devote resources to internal IT projects, it is common to anticipate that those employees will also be responsible for cyber security. This is a significant blunder since it may go against one of the most important concepts of cyber security: the separation of roles. Because it controls the data, information, and strategic direction, the organisation must determine the cyber security requirement. To translate the demand into technical policies, the IT department must follow best security practises. The human resources (HR) function must then provide employee training and education to fulfil the demand in collaboration with the IT and business functions. When the IT function is outsourced, there is a propensity to neglect or minimise the importance of effective cyber security in the outsourced contract, because people negotiating the contract may not have a thorough understanding of the requirement, or they may remove it because it is an unnecessary cost. When a security function is outsourced, it is frequently a kind of duty abdication rather than delegation. The guiding principle is that while organisations can outsource information security implementation and management, they cannot export ownership responsibility. The cost of establishing and implementing a cyber security framework that is enough to defend the organisation will be higher and securing capital or operating budget approval may be difficult. The capacity to design a strong cyber security strategy is somewhat dependent on the organization's grasp of information security risk management, which is not always the case. Organizations can also evaluate their cyber security capabilities using one of the Capability Maturity Models, which are commonly used in software development but have many similarities in the cyber security world.

In the information and cyber security areas, there are literally dozens (if not hundreds) of standards. Some are broad in scope and apply to a variety of security issues, while others are narrowly focused and only pertain to a single technology. There's also the risk that, especially for larger organisations, obtaining ISO/IEC 27001 certification means they're entirely secure and all they have to do now is 'keep turning the handle.' This is far from the truth, as complacency is frequently the cause of both organisations and individuals failing to notice a new threat or weakness and being successfully targeted as a result. Although there are several outstanding standards in the cyber security industry (most notably the US National Institute of Standards and Technology (NIST), BSI, and ISO/IEC standards), few of them are easily adaptable to SMEs. This is where the government of the United Kingdom's Cyber Essentials scheme shines. Implementation guidelines are also more suited to larger organisations, making it difficult for SMEs to adapt them to their specific circumstances. Many worldwide standards imply that organisations would have established some higher-level processes and procedures that many smaller organisations would not be able to do. Small businesses may not be able to commit to the degree of investment required to attain ISO/IEC 27001 certification.