CHAPTER 1: INFORMATION SECURITY AND CYBER SECURITY

The terms 'information security' and 'cyber security' are often used interchangeably, when in fact they refer to different (albeit related) things.

Information security is concerned with ensuring the confidentiality, integrity and availability (C, I and A) of all information held by an organisation, irrespective of whether the information is electronic or in hard-copy format. As a result, information security generally involves considering physical and environmental controls alongside technological ones (lockable filing cabinets, key-code doors, etc.).

Cyber security is a subset of information security and is concerned with the same things, but where information security takes a generalist approach, cyber security focuses specifically on electronic information (including the physical aspects of defending that information). New cyber risks emerge almost daily, and the successful organisation must do all it can to stay ahead of the curve.

Laws, regulations and contracts

The days of cyber security as an afterthought are long past. Today's organisations collect, use and store more information than ever before, and the global regulatory system is beginning to catch up.

The introduction of the EU General Data Protection Regulation (GDPR) in 2018 marked a major milestone for data protection and privacy laws across the globe. Most of us remember the flood of 'we need your consent' emails that arrived in our inboxes in the days leading up to (and after) the GDPR took effect, but those emails were only the tip of the iceberg.

The GDPR places a wide range of security and privacy obligations on organisations that process EU residents' data and

is supported by a regime of significant financial penalties (up to 4% of annual turnover or €20 million, whichever is greater). The Regulation also requires organisations based outside of the EU that process data on EU residents to appoint an EU representative, extending the reach of those obligations and penalties far beyond the EU's physical borders.

Another law that may be relevant is the Directive on security of network and information systems (NIS Directive). This places specific cyber security and business continuity obligations on digital service providers and operators of essential services such as power and water, with a view to mitigating the disruption that could occur as the result of a major cyber security incident.

While many organisations still grapple with the GDPR and NIS Directive, new laws such as the California Consumer Privacy Act (CCPA) or the Brazilian General Data Privacy Law (Lei Geral de Proteção de Dados Pessoais) are being introduced around the world, and further legislation is expected in the coming years. The increasing regulatory focus on data protection, privacy and continuity of key services inevitably leads to a greater focus on cyber security, as so much of the information held by organisations is in electronic formats, and the majority of essential services rely on electronic infrastructure.

It's not just laws that mandate effective cyber security. Cyber security obligations in contracts are increasingly common, as organisations begin to recognise the risks posed by information sharing between suppliers and partners. If your organisation takes card payments, for example, banks will expect you to adhere to the requirements of the Payment Card Industry Data Security Standard (PCI DSS), while many government contracts mandate a minimum level of cyber security to enter the tendering process.

CHAPTER 2: THREATS AND VULNERABILITIES

Risk is an inevitable part of life. Every time you do something in which the outcome is uncertain, you take a risk, whether it's something simple like crossing the road, or something complex like undergoing surgery. Risk is a function of uncertainty – without uncertainty, there is no risk.

Different business fields approach risk in different ways, but the general principles remain the same: the likelihood of an adverse event is mapped against the effect that event would have were it to occur. If the outcome is severe and the likelihood high enough, then it is sensible to take steps to protect against it – usually by reducing the damage caused by the outcome, or by reducing the likelihood that it will occur in the first place.

Cyber security risk derives from a combination of threats and vulnerabilities: vulnerabilities are exploited by threats to achieve certain goals, such as accessing a secure network or installing malware. This does not mean that cyber security risk is limited to deliberate actions by malicious actors – a leaky roof of a server room (vulnerability) can be 'exploited' by a rainstorm (threat), with potentially catastrophic results.

Threats and vulnerabilities can take many forms. A database that fails to properly sanitise user inputs, for instance, might be exploited by an attacker using an SQL injection to gain access to sensitive data, while unpatched software might allow an attacker to install malware, with any number of nasty results – wiping files or holding them to ransom, to name just two.

Software and hardware are always evolving, and the same is true for vulnerabilities – each advance brings new security challenges. Even longstanding, trusted software or hardware is not immune. In 2018, major computer chip manufacturers were stunned to discover that their processors had major security flaws (named 'Meltdown' and 'Spectre') at the hardware level

since 1995 – processors that are believed to be in almost every modern computer across the globe.[1]

Cyber threat actors come in all shapes and sizes too. While our first thought may be of the 'nerd' locked in a bedroom writing code for a prank, the reality is very different. Organised crime gangs, 'hacktivists' pushing a political agenda, and even state-supported actors all represent potential threats, irrespective of the size of your organisation.

Perhaps the most pervasive threat actor is something you can't live without – your employees. Even discounting 'insider threats' (the term used to describe employees who are actively looking to harm their organisation in some way, often because they are unhappy), many cyber security incidents are caused inadvertently by employees who lack awareness of the risks. According to a report by Verizon, 34% of data breaches in 2019 involved internal actors.[2]

Technical threats

When we think about cyber security, technical threats are usually the first thing that comes to mind. The news abounds with stories of vast data breaches that are eventually traced to some obscure vulnerability in hardware or software, and phishing emails carrying malware drop into millions of inboxes every day, all over the world. Every inch of progress towards security is a hard-fought battle, and to fight effectively, you need to understand the enemy's weapons.

[1] Samuel Gibbs, "Meltdown and Spectre: 'worst ever' CPU bugs affect virtually all computers", The Guardian, January 2018, *https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw*.

[2] Verizon, "Verizon 2019 Data Breach Investigations Report (DBIR)" *https://enterprise.verizon.com/en-gb/resources/reports/dbir/2019/summary-of-findings/*.

Malware

Malware has existed in one form or another since computers became commonplace. Self-replicating software was conceived in the 1940s, and one of the first viruses, known as Creeper, was created in the early 1970s, infecting US government computers and displaying "I'm the Creeper, catch me if you can" on the screen.

Since then, there has been an explosion of malware. Sites on the dark web offer a vast array of malware programs for sale, and new malware appears daily, taking advantage of the latest vulnerabilities in a never-ending arms race between the malicious actors who craft it and the cyber security professionals who defend against it. 'Malware' as a category encompasses a range of malicious programs, each of which operates differently.

Virus

Viruses are self-replicating programs designed to spread from computer to computer and deliver a payload. Viruses are not standalone programs – they are bits of code that need to be hidden in other programs to function and replicate. When the user runs the 'host' program, the virus infects the system and does its work.

Once it has infected a system, the virus has two goals: replicate itself as much as possible and deliver the payload – ideally without being spotted. Some of the earliest viruses were called 'boot sector' viruses, because they infected sections of a drive that are read when a computer is booted up, making them hard to detect, and were often spread through the sharing of floppy discs (which were still in common use at the time).

Some of the most common viruses of the Internet era are macro viruses – viruses written in the scripting language found in Microsoft® Office and embedded in Office files, such as Excel spreadsheets or Word documents. Opening the document allows the virus to infect the system, with potentially catastrophic results. Emails featuring infected Office documents have been a common attack vector since the early 1990s, so much so that

'don't open suspicious attachments' has become a cyber security maxim.

Worms

If the principal characteristic of a virus is that it is a self-replicating program that must be embedded in another program to function, then a worm is a virus with that limitation removed. Worms do not need to be embedded in other programs and can replicate without user interaction, making them especially dangerous.

One of the best-known worms in recent years is Stuxnet. Discovered in 2010, this highly complex worm targeted industrial control systems in an Iranian nuclear facility, changing the speed of uranium enrichment centrifuges until a large number broke from the strain. Commonly believed to have been developed by US and Israel intelligence agencies, Stuxnet is considered by some the world's first "cyber-weapon of geopolitical significance".[3]

Ransomware

Ransomware exploded into the public consciousness with the WannaCry attack on the NHS in 2017, which affected up to 70,000 devices including hospital equipment.[4] Other major organisations such as FedEx and Renault were also affected, along with a number of universities and government institutions across the globe.

---

[3] Holger Stark, "Stuxnet Virus Opens New Era of Cyber War", Der Spiegel, August 2011, *https://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html*.

[4] Robert Mendick, "Cyber attack on NHS would trigger full Nato response, says alliance's general secretary", The Telegraph, August 2019, *https://www.telegraph.co.uk/news/2019/08/27/cyber-attack-nhs-would-trigger-full-nato-response-says-alliances/*.

Ransomware is a payload, usually transmitted by self-replicating worms or Trojans, that encrypts or otherwise prevents access to the user's files until a ransom is paid (usually in Bitcoin). Some ransomware will take a copy of the user's files and threaten to publish them, but the effect is the same – pay up or lose out.

Before the 2017 WannaCry attacks (which occurred worldwide, not just in the UK), ransomware primarily targeted individual consumers. The 2017 attacks marked the beginning of a shift in focus, with 81% of ransomware attacks in 2018 targeting organisations, not consumers.[5]

Trojan horses

Trojan horses, or just 'Trojans', are a type of malware that pretend to be something else. The name comes from the ancient Greek story about the fall of Troy.

Trojans generally masquerade as legitimate programs to trick you into activating them, though some can spread on their own without user interaction. One of the most common attack vectors is email, as Trojans can be embedded in seemingly innocuous attachments such as spreadsheets or Word files. Once activated, the Trojan sends spoof emails to everyone in the address book, further spreading the infection.

Trojans can carry almost any kind of payload, but keyloggers and 'backdoors' that allow access to sensitive information or systems are common. Trojans that contain keyloggers or other methods of capturing information usually send the information to a master server from time to time; these transmissions can sometimes be the only way to identify that a Trojan is present.

[5] Symantec, "Internet Security Threat Report", Volume 24, February 2019, *https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf*.

Hybrid malware

Hybrid malware is malware that combines different aspects of other malware in order to be more effective.

Most of the malware we encounter today is a hybrid – for example, a worm with a ransomware payload, like WannaCry. Worms with Trojan or rootkit payloads are responsible for most 'botnets' – connected groups of computers or other Internet-enabled devices that are used to conduct distributed denial-of-service (DDoS) attacks, where a large number of devices communicate with the target simultaneously to overload it. Internet of Things (IoT) devices are particularly prone to botnet infections and related threats because they tend to have less effective security at both hardware and software levels (though this is beginning to change as awareness of IoT threats increases).

'Living off the land' and 'fileless' malware

A relatively recent development in the cyber threat landscape, 'living off the land' attacks involve the use of legitimate system and administrative tools (such as PowerShell or TeamViewer) that are already installed on the target system. These attacks can be difficult to detect, as the malicious activity blends in with other, legitimate administrative use of such tools.

A related concept is 'fileless' malware. Living off the land techniques are sometimes called fileless malware as they only involve existing, legitimate software and don't require, for example, the user to download an infected file. This isn't entirely accurate. Instead, fileless malware is better thought of as an attack that does not require or generate additional files that antivirus or anti-malware software might identify as suspicious. Examples include malware that runs and delivers its payload entirely within system memory, scripts embedded in the Windows registry system, and some browser-based cryptojacking attacks.

Defending against malware

Raise awareness

If employees don't understand cyber security and the role they play in protecting the organisation, even the best technical defences won't help. Training and awareness help employees recognise threats and take appropriate action.

Keep systems up to date

Software and hardware updates often include fixes for known vulnerabilities and should be applied promptly (e.g. through a patch management system) when they are made available by the vendor. Systems that are no longer supported by the vendor are a common factor in many data breaches and should be replaced or retired.

Deploy anti-malware tools

Antivirus and anti-malware software, firewalls and similar tools all help protect against malware. These programs should always be kept up to date to help protect against newly discovered vulnerabilities.

Secure backups

Taking regular backups has long been cyber security best practice, and backups are one of the best defences against ransomware – no need to pay a ransom if you can restore your files with a few clicks.[6] Some emerging strains of ransomware

[6] This is something of a simplification. While effective backups make it possible to recover from ransomware and similar attacks, that doesn't mean you should rely on the backups as the only means of defence. Malware (especially ransomware) can be difficult to remove, and the process of restoring your data from backups is necessarily time consuming, even for small organisations. It is far better to prevent the attack from occurring in the first place.

can infect or delete backups, however, making it more important than ever to ensure that any backup service has adequate information security measures, including antivirus and anti-malware tools.[7] Malware can remain dormant for long periods before triggering, so it is also important that backups are run frequently and retained for long enough to allow recovery in such an event.

Hacking

At the most basic level, criminal hackers find and exploit flaws and vulnerabilities in hardware and software. There is no shortage of flaws to find, either – no piece of software or hardware is truly immune, and new vulnerabilities are identified every day. Zero-day vulnerabilities (a vulnerability in newly released software or hardware that the manufacturer is not aware of) are a favourite target of criminal hackers, as attacks are more likely to be successful.

Criminal hackers are a disparate group encompassing everything from the stereotypical basement-dwelling nerd to state-supported 'hacker teams' with extensive financial backing and equipment. To better classify the threat posed by each type of criminal hacker, they are usually categorised as follows:

Script kiddie

This term refers to low-skilled, often young criminal hackers who use prebuilt tools to carry out low-sophistication attacks, usually without any real understanding of the underlying principles. While this doesn't make them any less threatening – the tools they use are built by skilled criminal hackers who know exactly what they're doing – it does mean that the vulnerabilities they exploit are usually common ones for which fixes may

[7] Lawrence Abrams, "Zenis Ransomware Encrypts Your Data & Deletes Your Backups", Bleeping Computer, March 2018, *https://www.bleepingcomputer.com/news/security/zenis-ransomware-encrypts-your-data-and-deletes-your-backups/*.

already be available, and against which basic cyber security measures offer protection.

A notable proportion of cyber crime occurs in exactly this way – inexperienced malicious actors purchasing simple tools or botnets to carry out low-level attacks that, despite their simplicity, still present a tenable threat to the organisation. Many attackers have little or no appreciation of the wider effects of their attacks or the principles that underpin them, in part because it is so easy to buy hacking tools and malware kits online. They have little concept of the real effect or cost of their attacks and will often claim that the attack was only done 'for the lols'.

Blackhats

Skilled criminal hackers who identify new vulnerabilities and develop the tools used to exploit them are known as 'blackhats'. Financial motivation is common – many blackhats sell the hacking tools they develop through online black markets, though they may also carry out attacks themselves in the hope of extorting payment (e.g. via ransomware) or selling stolen information to other criminals.

Unlike script kiddies, blackhats know exactly what they're doing and usually have a clear idea of what they want to achieve, making them some of the most effective and feared attackers.

Hacktivists

Hacktivist is more a classification of motivation than of skill or ability. Hacktivists carry out attacks to promote an agenda, though the ideology is often ill-defined and may vary over time. Hacktivist attacks are difficult to predict, not only due to the disparate nature of the groups themselves but also because of the wide range of potential targets. Notorious hacktivist group Anonymous, for example, has conducted attacks on the Church

of Scientology, Sony Online Entertainment, Islamic State and Donald Trump, to name but a few.[8]

State actors and cyber warfare

Cyber warfare may seem like something out of a science-fiction novel, but cyber attacks carried out by nation-state actors are increasingly common. In July 2019, Microsoft reported that it had notified almost 10,000 customers (84% of which were enterprise accounts) that they had been "targeted or compromised by nation-state attacks" over the course of the previous year.[9]

State-sponsored attackers often have access to extensive funding and equipment, and may operate with actual or tacit legal immunity in their country, making them very difficult to bring to justice. Nation-state attacks also tend to be highly targeted and focused on achieving specific goals, such as exfiltrating intellectual property or disrupting critical infrastructure. The 2010 Stuxnet attack on Iranian nuclear facilities (mentioned earlier in this book) is an infamous example of cyber warfare.

Ethical hacking

Not every hacker is a cyber criminal. Ethical hackers use the same tools and techniques as criminal hackers to search for vulnerabilities, but instead of exploiting them, they inform the system operator so that the vulnerabilities can be fixed. This approach, known as 'penetration testing', helps organisations

[8] Brian Feldman, "An Incomplete List of Every Person, Place, and Institution Upon Which Anonymous Has 'Declared War'", New York Magazine, March 2016, *http://nymag.com/intelligencer/2016/03/everything-upon-which-anonymous-has-declared-war.html*.

[9] Tom Burt, "New cyberthreats require new ways to protect democracy", July 2019, *https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/*.

identify and resolve vulnerabilities before they fall victim to an attack.

There are several types of penetration test. Two of the most common are external vulnerability scans, which highlight weak spots in how you connect to the Internet and other external systems, and internal vulnerability scans, which pinpoint weaknesses in internal networks that could be exploited by malicious insiders or external attackers who have managed to access them. Other types include web application penetration tests and wireless network penetration tests, which look for weaknesses in web applications or in your wireless networks; phishing simulations; and even physical entry tests that highlight weaknesses in the boundary of your premises that might allow an attacker to enter (e.g. via a social engineering attack).

Legitimate ethical hackers hold an internationally recognised certification and are subject to a strict code of conduct. The scope of testing is agreed with the client, ensuring no disruption to operational systems and services. Penetration testing services are used by organisations of all sizes, but are particularly useful for small and medium-sized organisations that do not have the in-house expertise to carry out such testing themselves.

Information security standards and frameworks, such as ISO/IEC 27001:2013 or the UK's Cyber Essentials scheme (among others), strongly encourage the use of penetration testing to highlight vulnerabilities for remediation.

Insecure configuration

Many technical threats rely on or take advantage of poorly configured devices to do their dirty work. Software and hardware are usually supplied in their default state, with preinstalled applications, default passwords and the like. This makes life easier for consumers, but it also creates risk for your organisation.

Preinstalled software is common on desktop and mobile devices, but each item of software presents its own risks. Default accounts and passwords, insecure transmission protocols, unexpected open ports and worse can arise simply because it's

the software's default setting. The same is true of more technical hardware, such as routers or server equipment. An attacker can purchase a list of default passwords for a particular device, and software that scans the Internet for those devices, then carry out attacks once a suitable device is found.

Preinstalled administrative tools pose a major risk, as they allow the user much more control than consumer-focused applications and can potentially enable more damaging attacks. Network and server configurations should also be a primary concern, as misconfiguration can be the gateway through which an attacker gains access to sensitive areas or information.

Applications for mobile devices often require permissions that are not strictly necessary to perform the task at hand, like access to microphones or cameras. Mobile devices often don't have antivirus or anti-malware protection installed either, making them especially vulnerable. Risks also arise if your organisation allows the use of personal devices to access secure networks or files, or allows users to freely install software.

It is far easier to begin from a state of secure configuration than to apply one retrospectively. The first thing to do is to take an inventory of all hardware and software so you know what you're dealing with. Once you've done this, you can develop secure baseline configurations that define the permitted software, hardware and necessary security-hardening steps to ensure security. Those steps might include changing all default passwords, limiting administrative tools to authorised, secure administrative accounts, disabling default accounts, or removing unnecessary software or peripherals. Your baseline should also include antivirus and anti-malware software as standard on all systems, including mobile devices.

You should also configure servers and networks with intrusion detection software so you can monitor suspected attacks. Instead of having one big network that everything connects to, segment it to make it harder for unauthorised users to access sensitive data or systems (especially where the network connects to payment systems such as point-of-sale devices, etc.). Network, server and database access channels should employ brute-force

password protection (where login is disabled for a time after a set number of failed attempts) to defend against bulk password attacks.

One common configuration issue is inadvertent information disclosure, where HTTP headers and standard system responses provide information that would be useful to attackers, such as software names, version numbers and other information that a malicious actor could use to craft more effective attacks. Protect against this by disabling or modifying HTTP response headers and system responses so they do not disclose identifiers.

Password reset functions are another area in which information disclosure is common. If your password reset function confirms whether the login information entered is in use or not in use (e.g. 'this username is not recognised'), then it is possible for an attacker to enumerate a list of usernames that could later be used to attack the system. To prevent this, configure password reset functions to return a generic message (e.g. 'if you are a registered user, a password reset email will be sent') regardless of whether a recognised or unrecognised username is entered.

Once you have defined your baseline configurations, implement controls that prevent users installing their own software or making other potentially harmful changes. Develop a patch management policy that ensures patches and updates are applied promptly (e.g. within two weeks of release), and a change management procedure so that any future changes to the baseline configuration are assessed for risk and suitability before they are implemented.

Once you have defined and rolled out your configurations, consider using periodic vulnerability scans to identify any weak spots you might have missed. Even the most comprehensive baseline configuration may still contain weaknesses, and new vulnerabilities arise daily – it's better to stay ahead of the game than to learn the hard way.

CHAPTER 3: SECURITY BY DESIGN

For a product (whether software or hardware) to be secure, it must be developed with security in mind from the outset. This was a challenge in the days when most development still used the 'waterfall' model; in the era of Agile and similar, more iterative methodologies, the challenge has never been greater.

Secure development is not a new concept. The rapid spread of computers and the Internet in the late 1990s highlighted the myriad security flaws and issues in the era's operating systems, software and hardware. Viruses and worms proliferated, and customers demanded action. At Microsoft, Bill Gates's famous 2002 'Trustworthy computing' memo outlined the need for security to become an intrinsic aspect of computing, such that Microsoft products would be seen to be as safe and reliable as the water or electricity supply.[10]

As a result, Microsoft developed the Security Development Lifecycle (SDL).[11] Adopted by Microsoft in 2004 and applicable to third-party developers as well as Microsoft's own, the SDL laid the foundation for secure development methodologies. In 2008, Microsoft made information on the SDL available free of charge, and it was quickly adopted and adapted by a wide range of industries.

Secure development methodologies are now well established, yet far too many organisations still consider security something that can be 'bolted on' late in the development process. Such an

[10] Bill Gates, "Bill Gates: Trustworthy Computing", Wired, January 2002, *https://www.wired.com/2002/01/bill-gates-trustworthy-computing/*.

[11] Microsoft Security Development Lifecycle, Microsoft, accessed October 2019, *https://www.microsoft.com/en-us/securityengineering/sdl*.