Protecting your ideas

IP Community Guide to Cyber Defence

www.ipcybersecurity.co.uk

Cyber Defence

1. Scope of "Cyber Defence"

Recently there has been much public debate about measures that companies can lawfully take to protect their computer networks and data. The discourse has at times been hindered by the use of varying, overlapping, or confusing terminology.

2017 marked the year of the most disruptive cyber incidents to date, with ransomware campaigns like WannaCry and Petya/NotPetya crippling organisations globally, a serious increase of data breaches affecting large and small companies alike and an increase in exploits targeting business and government networks. The threat landscape remains complex and ever-changing, ranging from organised crime, opportunistic threats and hacktivists to foreign intelligence agencies and malicious or accidental insider risks. Companies may lawfully take a variety of actions to protect their computer networks and data but the discourse around such measures has at times been hindered by the use of varying, overlapping or confusing terminology. The current environment represents challenges for companies with global supply chains that fall into numerous jurisdictions, increases legal uncertainties and hampers the standardisation of nomenclature across the cyber defence industry.

Lawful cyber defence protections can generally be categorised along a spectrum ranging from passive defence to active cyber defence (ACD) measures, a term first coined by the U.S. Department of Defense in 2011. ***Passive defence*** is aimed at securing one's own systems and network and includes measures that every company should adopt as minimum cybersecurity standards, such as basic security controls, firewalls, patch management or network scanning and monitoring (See Section 6).

In the UK, ***ACD falls under the DEFEND element of the UK National Cyber Security Strategy 2016-2021***, which aims to ensure that UK networks, data and systems in the public, commercial and private spheres are resilient to and protected from cyberattack. The strategy defines ACD measures as cyber protection measures that, help security analysts understand threat actors and threat landscapes in order to devise *proactive* steps to combat and defend against them. Government objectives in undertaking ACD include increasing the scope and scale of Government's capabilities (Ministry of Defence[1], NCA, GCHQ[2]) to respond to and disrupt state-sponsored and criminal cyber activity targeting the UK and to defeat the vast majority of high-volume/low-sophistication malware activity on UK networks by hardening the overall cyber defence of UK businesses and cyberspace more broadly.

A key strand in delivering the strategy's objectives is the National Cyber Security Centre's (NCSC) Active Cyber Defence programme, launched in November 2016 and aimed at tackling high-volume commodity attacks rather than highly sophisticated and targeted attacks. In short, the ACD program attempts to proactively address the majority of

[1] Note the creation of the Joint Forces Command (JFC) Cyber Reserve Force (CRF), made up of experts from Army, Navy and Air Force Reservists, which is specifically designed to help the UK utilise individuals cyber security skillsets in the protection of the UK and its interests worldwide.

[2] Note the creation of the National Cyber Security Centre (NCSC), which brings together expertise from CESG (the information assurance arm of GCHQ), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure, to help protect UK critical services from cyberattacks, manage major incidents and improve the underlying internet security of the UK through technological improvement and advice.

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

cyberattacks before they even reach users. In collaboration with UK industry and public sector organisations, the ACD programme offers active measures like Takedown Service (removal of phishing sites, notifying hosting providers of malicious content) or DMARC, a technique that authenticates government and private domain emails, thereby making it harder for cyber criminals to spoof users through illegitimate email addresses and messages.

Whilst there is currently no comparative to the UK's ACD programme in the U.S., a lively debate about ACD measures has been underway on the other side of the Atlantic for several years.

A 2016 Project Report prepared by the Center for Cyber & Homeland Security at the George Washington University defines ACD as a spectrum of proactive cybersecurity measures that fall between traditional passive defence and offence which may range from low impact/risk to high impact/risk activities. Active defence is not considered 'hacking back' and the terms should not be used interchangeably. See section 5 of this Guide for a detailed look at 'hacking back' and its legal implications.

The report shines a light on the legal "grey zone" companies in the U.S. currently find themselves in when thinking about ACD measures and formulates two key recommendations for U.S. lawmakers: The U.S. Justice Department should issue guidance about what kinds of ACD measures are permissible under U.S. law; and the Department of Homeland Security ought to establish collaboration procedures with private sector companies that wish to implement ACD actions. ***The following ACD measures are equally appropriate for SME clients operating within the UK***:

On the low-risk spectrum of ACD, companies and other cyber defenders may share actionable cyber threat indicators, mitigation tools and resilience strategies to improve their defensive capabilities.

SMEs can use the information and advice provided by the NCSC as a key resource to gain a better understanding of the threat environment their business faces. The NCSC regularly issues alerts to address and inform about cyber threats which are detected in the UK. The free service also includes in-depth analysis, sector-specific reports and assessments on cyber threats, the latest malware and known vulnerabilities.

As another low-risk defensive technique, companies may prevent cyber threat actors from reliably accessing valuable data and files by intentionally mixing it with false information or otherwise using other deception technologies (see our ***SME Guide to IP Cybersecurity***). SMEs can enable such denial and deception techniques on their networks through a trusted network administrator at relatively low cost. Other tools, such as tarpits, sandboxes or honeypots, though slightly more sophisticated on a technical level, can slow down hackers and allow a computer security expert to observe the hacker's attack techniques. This information can then be used to improve cyber defences on the organisations' actual network.

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

Hunting, which consists of rapid actionable procedures and technical measures that detect and remove hackers already present in a defender's network remains a low-risk and highly effective cyber defence measure. However, technical knowledge is required for this type of ACD and given IP Wales' research in this area[3], which reveals the lack of SME resources dedicated to cybersecurity activities, it therefore remains an uncommon technique for most SMEs.

Moving along the active defence spectrum, human intelligence techniques such as covert observation, impersonation and misrepresentation of assets in the Deep Web/Dark Net may be used to attract malicious cyber actors in order to gather intelligence on their motives, activities and capabilities. Larger organisations now regularly feature such in-house cyber intelligence teams that analyse intrusions, and research and collect data in the Deep Web/Dark Net to turn it into useful intelligence on the threat landscape their business or client faces. Should SME clients choose to incorporate such defence measures, they are advised to outsource these to external consultants, given that the specialist nature of this work is likely to be beyond the competence of the majority of SMEs.

In order to remain within lawful boundaries, both hunting and human intelligence techniques must remain strictly defensive in nature and cannot be used to disable or attack the hacker.

Other high impact/risk activities, such as taking down botnets (large number of malware-infected and compromised computers) or coordinating sanctions, indictments and trade remedies to impose costs on malicious cyber actors are both significantly more complicated on a technical level and also require close cooperation with government.

In October 2017, the bipartisan Active Cyber Defence Certainty (ACDC) Act was introduced by U.S. lawmakers, aimed at amending the Computer Fraud and Abuse Act (CFAA) to allow companies to go into networks outside of their own to gather intelligence or even to destroy data which was stolen from them. The draft legislation is currently on hold as it faces technical, legal and policy scrutiny.

The ***Tallinn Manual 2.0*** on the International Law Applicable to Cyber Operations, a research project commissioned by the NATO Cooperative Cyber Defence Centre of Excellence, does not specifically address how non-state entities, including the private sector, may or may not choose to protect their networks or which ACD measures private companies can deploy. However, the group of international legal experts commissioned by NATO conclude under Rule 33 that "non-state actors are not entitled to engage in the responses that states may conduct under the law of State responsibility when facing hostile cyber operations by or attributable to other States." At the same time, however, the scholars posit that, "States enjoy the authority to establish specific legal regimes governing cyber operations by non-state actors and cooperative arrangements may be set up to address particular cyber issues."

[3] Report prepared for the Welsh Assembly on IP Infringement & Enforcement Issues (2011)

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

Cyber defence is also part of NATO's core task of collective defence, with the treaty organisation affirming that international law applies in cyberspace, recognising cyberspace as a domain of operations in July 2016. Over the last two years, NATO has continually intensified its cooperation with industry through the NATO Industry Cyber Partnership, including on several objectives which fall within the ACD spectrum, such as sharing of best practices and information on threats and vulnerabilities.

It is likely that private sector companies will increasingly work together to develop industry standards and best practices in the realm of ACD measures. While all ACD techniques may be useful in protecting data and networks, businesses should keep their individual return on investment in mind to make sure their cyber defence investments are not off-balance. ***For SMEs, it is generally recommended that network security architecture and passive defence techniques should comprise the vast majority of their cyber defence investment.*** Where appropriate, SMEs should consider ACD measures on the left side of the spectrum. Activities on the rightmost extreme of the active defence spectrum should not be viewed as a priority for SME clients.

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

2. Cyber Threat Intelligence Gathering as Cyber Defence Activity

Cyber defence activities encompass a range of tools and techniques, from passive preventive measures intended to prevent or deter malicious cyber activity to more active/offensive actions taken in response to a particular cyber threat.

A 2017 Cybersecurity Landscape Report by Control Risks (a specialist Global Risk Consultancy) identified that companies in the UK are increasingly concerned that their organisation will suffer a cyberattack. At the same time, these organisations struggle to effectively assess cyber risk to their business and turn it into effective mitigation strategies.

Cyber threat intelligence (CTI) gathering has emerged as a key element of a cyber risk mitigation strategy for the private sector, a term falling into the spectrum of proactive strategic and technical cybersecurity measures companies may consider taking to protect their data and networks. Moving beyond passive defence, active defence includes a range of both low impact/risk and high impact/risk activities, as detailed by a 2016 Report by the Center for Cyber & Homeland Security at the George Washington University (see Section 1).

CTI is based on a variety of intelligence collection vectors, such as open source intelligence (OSINT), social media intelligence (SOCMINT), human intelligence (HUMINT) and technical intelligence. Most commonly, CTI finds application in researching and analysing cyber threat trends and the behaviour of known cyber threat groups in the areas of cybercrime, cyber espionage and hacktivism (groups or individuals seeking to promote a political and social agenda). CTI services are increasingly offered to help organisations understand and manage business risk, but products can vary enormously in their scope, applicability, aims and content. According to a 2015 MWR InfoSecurity Report, it is therefore critical for businesses to consider tailored CTI products and services should they choose to incorporate them into their cyber risk management procedures.

In the UK, SMEs may benefit from intelligence and information exchange on cyber threats by joining the Cyber Security Information Sharing Partnership (CiSP), a joint government and industry initiative. Launched in 2013 as a key component of the UK Cyber Security Strategy, CiSP introduced a free virtual collaboration environment for government and companies to exchange information on threats, attack and reconnaissance methods, vulnerabilities and mitigation strategies in real time, thereby increasing their situational awareness and reducing the impact of cyber threats on UK businesses.

According to the NCSC, the information exchange includes not only tactical intelligence such as attack methodologies and tools but also technical indicators of specific malicious software and the attack vectors it is distributed through. CiSP members also enjoy access to free network monitoring reports tailored to their organisations' requirements.

All UK-registered companies or legal entities responsible for the administration of an electronic communications network in the UK are eligible to become CiSP members. CiSP guarantees full confidentiality of the names of the organisations involved and the information exchanged between them, thereby lowering reputational risks. Apart from increasing the situational awareness of UK businesses, CiSP can empower organisations to

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

understand cyber threats within their context, thus fostering a more proactive and strategic cybersecurity posture and defence.

Various industry groups and sectors have also rolled out more informal information sharing platforms, such as via a forum or simply an email list. These may also be helpful but best practices indicate that more secure (verified) groups result in the most effective CTI sharing.

The IP Wales Online Initiative (see www.ipcybersecurity.co.uk) has benefitted greatly from working closely with the two cybersecurity clusters in Wales (North & South)[4], comprised of informal groups of small companies from the region who actively work in cybersecurity. Although managed independently, these form part of a UK network who collaborate and communicate through the UK Cybersecurity Forum to ensure that opportunities and best practice are shared nationally. Membership is free and offers client SMEs the opportunity to hear speakers and take part in networking and discussion.

[4] Linked with Global EPIC, a partnership in innovation and cybersecurity for conflict, crime and security research which seeks to strengthen collaboration between regional ecosystems.

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

3. Providing Legal Certainty

Because defensive cyber actions can raise a variety of legal issues, SME Clients may wish to consult with their lawyers before conducting some types of defensive cyber activity.

Providing legal support to furnish clarity of thought and action by a business client needs to be multidisciplinary (employment, corporate & commercial, intellectual property, data protection, dispute resolution) and holistic (IT forensics and cybersecurity, cybersecurity insurance, PR).

PwC's 2014 Global Economic Crime Survey identified the main threat to a client business as coming from an insider. Employment lawyers can advise on the adequacy of client's standard terms of employment and internal policies (including the monitoring of employees) to protect against insider security risks.

Corporate & commercial lawyers can audit supply contracts to advise on any security risks. They can also advise on software licenses and service contracts associated with IT security (including managing cybersecurity incident response & data recovery), as well as international and national regulatory compliance e.g. Directive on Security of Network and Information Systems (NIS Directive). Advice can also be offered on the reputational management from the fallout of a cybersecurity breach.

IP lawyers can help identify, prioritise and protect trade secret data, and otherwise in a post-breach scenario advise on the possibilities of preventing further dissemination of trade secret data. How a client business protects its trade secret data is important not only in the practical way of reducing or preventing 'digital misappropriation' but also because legal protection of trade secret data demands that the victim has taken "reasonable efforts" or "reasonable steps" to maintain the secrecy of the data at issue. Case law from the U.S. has already seen courts assessing the "reasonableness" of a companies' cybersecurity in terms of identity and access management (password protection, 'need to know' access, secure server storage); data security measures (USB use restrictions, distribution controls); perimeter and network defences (firewalls, data encryption, online use restrictions); communication (pop-up warnings) and monitoring (email monitoring).

Data protection lawyers can advise on the suitability of measures to protect customer information and other personal data under the General Data Protection Regulation (GDPR).

Dispute resolution lawyers can advise on potential liabilities resulting from breaches as well as which parties clients can seek to recoup losses from. They can also assist with private prosecutions against the perpetrators of the security breach.

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

4. Conducting Defensive Cyber Action in a Global Environment

SME Clients may rely upon cloud computing and/or form part of a supply chain extending over multiple countries with differing legal regimes.

International Norms

Governments increasingly desire rules for predictable state behaviour in cyberspace. Whilst states generally agree that a debate on cyberspace and its effects on the foundations of international security is needed, opinions on global norms and best practices in the digital realm continue to diverge for a number of political, economic and strategic reasons.

Since 2004, a UN Group of Governmental Experts (UN GEE) has sought to expedite international norms and regulations to create confidence and security-building measures between member states in cyberspace. In a first major breakthrough, the GGE in 2013 agreed that international law and the UN Charter is applicable to state activity in cyberspace. Two years later, a consensus report outlined four voluntary peace time norms for state conduct in cyberspace: states should not interfere with each other's critical infrastructure, should not target each other's emergency services, should assist other states in the forensics of cyberattacks, and states are responsible for operations originating from within their territory.

The latest 2016-17 round of deliberations ended in the stalling of the UN GGE process as its members could not agree on draft paragraph 34, which details how exactly certain international law applies to a states' use of information and communications technology. While the U.S.A. pushed for detailing international humanitarian law, the right of self-defense, and the law of state responsibility (including the countermeasures applying to cyber operations), other participants, like China and Russia, contended it was premature to determine specific language for the guidelines. The current debate revolves around continuing the GGE process as an open-ended working group or transferring it to a new UN committee for cyber norms.

In May 2018, UK Attorney General Jeremy Wright outlined Britain's position on applying international law to cyberspace (the first time a Government Minister set out the UK view on record and outside of the UN GGE context). Wright reexamined existing UK positions on the UN Charter to cyberspace, such as the applicability of articles 2(4) (prohibition of the use of force), 2(7) (non-interference in internal affairs), and 51 (inherent right of self-defense). The Attorney General also stressed that public attribution of a cyber incident to a state actor would not only be a legal matter, but equally a political decision.

Other avenues to further advance global cyber norms are also underway. The Tallinn Manual Process, prepared by an international group of legal experts and facilitated by the NATO Cooperative Cyber Defence Centre of Excellence, has put forward two comprehensive academic editions of how existing international law applies to cyberspace. The Manuals do not represent the views of NATO or any other state but given their authoritative context, though through a decidedly Western lens, they may well have an effect on how states formulate their views in the cyber policy debate.

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

In early 2017, Brad Smith, Microsoft President and Chief Legal Officer introduced his company's ambitious proposal for a Digital Geneva Convention. The Convention would see states avoid launching cyberattacks which target intellectual property, critical infrastructures, or the private sector. At the same time, it calls on the tech sector to operate as a "neutral Digital Switzerland," and not conduct offensive operations against customers regardless of their country of origin[5]. Lastly, an independent non-governmental organisation would investigate and attribute offensive cyberattacks to specific state governments. Given the difficulties between public and private sector cooperation in cyberspace, in addition to the lack of global agreement between states, the Digital Geneva Convention will likely remain nothing more than an ambitious proposal for now.

A third, and arguably more likely approach could see states move more toward narrowly tailored initiatives for assurances in cyberspace. The 2015 cyber agreement between the U.S. and China concerning economic espionage and the theft of intellectual property remains one of the most effective deals falling into this category. Such a path offers opportunities for states to find common ground on specific security and economic interests without having to reconcile their starkly differing opinions on larger cyber governance concerns. A growing number of bilateral and multilateral agreements are slowly putting forward declarations of mutual interests and concerns or are establishing confidence and capacity building measures for cyberspace.

National

The divergence in trade secret laws across legal jurisdictions and difficulties in achieving effective legal enforcement makes trade secret protection a complicated issue for client businesses operating globally or as part of a global supply chain. A client business may therefore need to familiarise itself with the disparate laws of several countries.

In addition to familiarity with Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, doing business in the UK involving "personal data" will require compliance with the EU General Data Protection Regulation (Regulation (EU) 2016/679)(GDPR). The UK Network and Information Systems Regulations 2018 implement the Cybersecurity Directive ((EU) 2016/1148) (also known as the Network and Information Security Directive or NIS Directive) which applies to the operators of essential services [OES] (such as transport, health and energy) and to digital service providers [DSP] (such as online marketplaces, search engines and cloud services) – other than DSPs considered micro and small enterprises. The UK government omitted banking and financial market infrastructures under OES as equivalent provisions will exist elsewhere and introduced thresholds to capture only the most significant OESs in a particular sector. Like the GDPR, the NIS Regulations impose security and incident reporting requirements, but their focus is on the security of IT systems rather than the personal data processed by those systems.

[5] "Brad Smith takes his call for a Digital Geneva Convention to the United Nations", Microsoft On the Issues (The Official Microsoft Blog) Nov 9, 2017

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

Doing business in the U.S. requires a familiarity with the Defend Trade Secrets Act [DTSA], which was passed by Congress in 2016 to effectively federalise U.S. Trade Secret Law. This Act has application to trade secrets used in, or intended for use in foreign commerce, so client businesses operating with a U.S. counterpart face an additional risk management concern. Section 4 of the Act places an obligation on the U.S. Attorney General to report to Congress on the 'Theft of Trade Secrets Occurring Abroad'. The U.S. criminal counterpart to DTSA is the Economic Espionage Act [EEA], Section 7 of which makes clear that the statute applies to conduct occurring outside the U.S.A.

Whereas trade secrets may enjoy legal protection in some jurisdictions the same cannot be said of all. India, Malaysia, Singapore and Hong Kong for example do not provide for statutory protection of trade secrets or confidential information. Brazil has criminalised trade secret theft but the remedies for breach are considered to be limited. Criminal and civil litigation in China very rarely provides for the trade secret protect of foreign business and, along with Russia and Pakistan, China has been identified as having the worst reputation amongst global business for pursuing or investigating security incidents involving breaches of corporate data, with a suspicion that the government may be condoning, facilitating or even participating in trade secret theft.

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

5. 'Hacking Back'

More aggressive defensive cyber actions — sometimes called 'hacking back'/'Offensive Cyber'/'legal right to bear cyber arms' — have been central to the ongoing legal and policy debate over measures that companies should and should not be permitted to conduct in defence of their networks and data.

Retaliatory hacking by a client business is likely to be deemed illegal in the UK under the Computer Misuse Act (CMA) 1990, which makes it a criminal offence to gain unauthorised access to a third party's computer or data or otherwise impair the operation of a third party's computer e.g. through orchestrating a retaliatory DDoS attack (see our ***Guide to SMEs Reporting IP Cybercrime***).

However, the UK Government has introduced new legislation to 'clarify' that GCHQ, Intelligence Officers and the Police possess the lawful authority to engage in hacking (pre-emptive or retaliatory) without criminal liability - thereby ensuring the "Offensive Cyber" capabilities set out in the National Cyber Security Strategy 2016-2021. Section 44 of the Serious Crime Act 2015 amends section 10 of the CMA and is intended to remove any ambiguity in the 1990 Act against the lawful use of powers to investigate crime.

It is reported the UK Government is already targeting computers in other countries being used for cyberattacks, particularly if there is no possibility of prosecution or for co-operation with authorities where the hackers are based. Ciaran Martin, Chief Executive of the UK National Cyber Security Centre (NCSC) states, "in the most serious cases, we have lawful powers where we can go after the infrastructure of adversaries – the infrastructure that people use to attack us – and we would do that in some of the most serious cases several dozen times a year."

In the U.S. the debate is currently focussed on whether businesses themselves should also be exempted from prosecution under the Computer Fraud and Abuse Act for taking cyber defence measures, such as 'hacking back'. The Active Cyber Defense Certainty Act (a discussion draft Bill currently referred to the Congressional Subcommittee on Crime, Terrorism, Homeland Security, and Investigations) seeks to offer protection to a 'hack' victim when accessing the computer of the attacker: to gather information in order to establish attribution of criminal activity to share with law enforcement; or to disrupt continued unauthorised activity against the victim's own network; or monitor the behaviour of an attacker to assist in developing future intrusion prevention or cyber defence techniques. However, the proposed Bill imposes limitations which include prior notification to the FBI National Cyber Investigative Joint Task Force and taking steps to prevent damage to intermediary computers not under the ownership of the attacker.

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

6. Effective Cyber Defence Actions

The spectrum of activities that can be initiated to protect a network and data is broad.

The theft or misappropriation of trade secrets can have a devastating effect on a company's competitiveness, financial standing and reputation. The loss of trade secrets may also result in third-party liability exposures with costly compensation claims.

According to a March 2018 study by Bromium (a virtualization technology company), IP theft ranges around US $500bn annually. A key priority for companies whose business depends on trade secrets lies in implementing effective cybersecurity measures to protect their most valuable assets. Cybersecurity protection also has legal relevance, as such measures have to be specifically considered by courts in the UK and elsewhere when assessing whether a company has taken adequate, or 'reasonable steps' to protect its trade secrets from theft or misappropriation. As internet use and cloud storage grows further, it is reasonable to expect that the specific type of cybersecurity measures and standards a company implements will play an increasingly important role in future trade secrets litigation.

The spectrum of activities that can be initiated to protect a network and data is broad. Initially, it is helpful for a business to understand what its key trade secrets are and what protective measures can be applied to them. In the UK, the NCSC *Cyber Essentials* are currently widely regarded as the minimum cybersecurity standards companies should follow to guard against the most common cyber threats. Adopting these best practices is also an easy way to publicly demonstrate an organisation's commitment to cybersecurity. ***Cyber Essentials include five technical controls every organisation should put in place to enhance its network defences:***

The first step is by using a firewall which allows for monitoring and control of network traffic, by allowing or disabling traffic based on a set of predefined rules. This may be used to control traffic moving in and out of a network or to control which areas of a network traffic can access. Cyber Essentials focuses on external or internet facing firewall(s). This first line of defence establishes a barrier between trustworthy secured or internal networks and untrusted outside networks (such as the Internet), thereby screening out hackers, viruses, and worms. For small-office networks with several connected devices, it is recommended to establish a dedicated boundary firewall around the entire network in addition to a software firewall, which helps prevent the spread of a virus within a network if one of the devices is infected.

Secondly, ensure that newly purchased devices and software are running on the most secure settings. Manufacturers and vendors frequently sell their products with default usernames, passwords and configuration settings still in place, making them vulnerable to unauthorised access. In addition to making the relevant changes on newly purchased devices and software, such as routers, wireless access points or firewalls, it is strongly recommended to use two-factor authentication (2FA). 2FA requires you to enter a code, commonly sent to your smartphone in addition to your password when accessing critical accounts and services such as email, banking and IT administration.

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

Implementing data and network access controls and restrictions are a third key way to reduce the potential damage of an account misuse or network breach. This is particularly critical for trade secret protection as trade secrets are not only threatened by outside hackers but often taken by departing employees. It is estimated that 80% of trade secret thefts involve present or former employees, vendors or customers. Controls should ensure that staff only have the access to the software, settings, and the online services required for their role. This includes network administrators, who should have a regular user account for day to day activities such as email and web browsing. Additional access privileges should only be extended when performing a specific task requiring it.

Fourth, protect an organisation from malicious software and viruses found on the operating system by enabling anti-malware programs or by purchasing additional anti-virus software packages. A network administrator may also create a list of applications allowed on company devices, effectively whitelisting and blocking other apps not found on this record. If possible, use apps that support Sandbox, a special security feature which allows an app to run in an isolated environment and therefore limits access to files and the system.

Lastly, ensure that all the organisation's devices, apps and software are kept up to date. Regularly applying security patches (update fixes of known security vulnerabilities) is one of the most important measures to improve an overall cyber defence posture. Cyber Essentials requires that all security patches are applied within 14 days of release. Should a manufacturer cease to release new updates for a certain product, consider a new replacement.

A number of additional cyber defence measures are useful for organisations seeking to protect their IP and trade secrets. Data encryption, strong password policies or storing sensitive data on an external hard drive can help prevent unauthorised remote access. Employees represent the most vulnerable entry point to a cybersecurity scheme and increasing their cybersecurity awareness through regular training, for example through simulations of phishing attacks, can go a long way towards addressing this vulnerability. Requiring digital logs whenever employees copy, print or relocate sensitive information or the use of swipe cards to access sensitive files on a network can help detect their improper access or removal. Lastly, pieces of software called Beacons may be deployed or hidden in critical data and files that, when taken from a system without authorisation, alert the defender of the intrusion and can even inform defenders about the structure and location of the foreign computer system if the file is removed.

Cybersecurity protections should not be viewed as static or a one-off effort because technology and cyber threats continuously evolve and advance. Depending on changing company goals or business practices, such protection measures should be continuously monitored, measured and adapted over time. More broadly, cybersecurity protection measures are most effective when closely interrelated and linked to other risk management policies. Cybersecurity experts regularly stress the need for holistic risk management and assessment policies for network and data protection.

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

One of the hard truths derived from a realistic threat assessment is it is currently difficult for companies to effectively defend themselves against a resourceful and highly capable cyber threat actor. These so-called Advanced Persistent Threats (APTs) may include well-resourced state actors or individuals and groups which will dedicate advanced skills and significant periods of time to research and execute attacks against their targets.

This makes it all the more important for SME clients to have incident response and contingency plans in place before any cyber breach occurs (see our ***Guide to SMEs Outsourcing Cybersecurity Incident Response & Data Recovery Activities***) and report such breaches if the SME client seeks a potential UK Government ACD response (see our ***Guide to SMEs Reporting IP Cybercrime***).

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.

Further Reading

This Guide is intended for educational use only and is *based upon issues discussed at the Center for Strategic and International Studies (CSIS) / Cybersecurity Unit of the U.S. Department of Justice (Criminal Division) Active Cyber Defense Experts Roundtable 10th March, 2015*:

National Cyber Security Centre Cyber Essentials

Tallin Manual 2.0 on the International Law Applicable to Cyber Operations (2nd Edition, 2017)

UK Government National Cyber Security Strategy 2016-2021

The Protection of Data in our Digital Age [2017] Journal of Business Law, Volume 6, 2017 p. 461

U.S. Active Cyber Defense Certainty Act

UK Computer Misuse Act 1990

United Nations Office for Disarmament Affairs. Developments in the field of information and telecommunications in the context of international security (un.org)

The Importance of Cybersecurity for Trade Secret Protection: Developments in trade secrets cases and the growing role of the NIST Framework (CREATE.org)

Trade Secret Theft: Managing the growing threat in supply chains (CREATE.org)

Project on Active Defense by the Private Sector against Cyber Threats from the Center for Cyber & Homeland Security (CCHS) at the George Washington University

The authors would like to thank Jason Davies (North Wales Cybersecurity Cluster) for his kind assistance when writing this Guide, any errors contained herein remain our own.