Cyber Security

For Small Business

Thomas Hayes
BA Hons, FBCS, CITP, FIP, CIPM, CIPP/E, MAPM

Cyber Security for Small Business

Email: thayes@hayesltd.com

Website; www.hayesltd.com

Contact Telephone: 07834 039328

Hayes Associates offers the following services:

- Data Protection & GDPR Advice
- Data Protection & GDPR Audits
- Cyber Security Audits & Advice
- Data Breach Management
- Subject Access Request Management
- Information Management Consultancy
- Cyber Essentials Accreditation
- ISO 27001 Accreditation
- Data Protection Officer (DPO) as a Service
- Data Protection and Cyber Security Training & Awareness - all staff levels

Introduction

If you spend more on coffee than on IT security, you will be hacked . What's more you deserve to be hacked

- Richard Clarke, author and former Special Advisor for Cyberspace to the US President

Data has been described by The Economist magazine as the most valuable resource on earth – even more so than oil. Ensuring that this data is protected is therefore an extremely important part of any organisation's objectives. This is especially so for any organisation that handles sensitive personal, or financial data. For a small business that does not have a lot of resources to invest in sophisticated IT infrastructure and cyber defences, this problem of protection is a significant one.

The short eBook will inform you as to the importance of Cyber Security from both the perspective of regulatory compliance and ensuing business continuity. It is aimed at small businesses that may not have the luxury of access to a great deal of expertise. The contents therein are not intended to be a full discourse on the whole range of topics that constitute Cyber Security. We trust however, that some level of awareness will result.

The eBook is offered freely without having to sign up to anything or receive any marketing emails or phone calls. It is one of a number in a series on data protection, the GDPR and Cyber Security. All are written for information and awareness.

GDPR

The General Data Protection Regulation (GDPR) is the latest in a series of data protection legislation that passed into law on 25th May of 2018,, replacing the previous Data Protection Act of 1998 (DPA98). It is a European Union Regulation that consists of 11 Articles and 99 Chapters and set out across 88 pages of text. The purpose of GDPR is to consolidated standardise across the EU countries, whilst adapting to meet the demands of the new technological era.

There are three specific mentions of Information Security in the GDPR. Cyber Security relates to the electronic data component whereas Information Security is a wider definition that also includes paper records Obviously, electronic data is by far the largest component of information these days. These rules ion the GDPR need to be considered from a cyber security perspective. Security is included as one of the seven principles that form the basis of the Regulation.

the principle of Information Security also underpinned previous data protection initiatives. For example, it was also included in the previous DPA98. Hence security – and thereby cyber security specifically, is a legal obligation. The principle set out in Article 5(1) (f) of the GDPR states that; Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality' It should also be noted that the Common Law Duty of Confidentiality also by definition, requires information security.

GDPR and Cyber Security

The Regulation does not mandate a specific set of cyber security measures that should be implemented. Compliance is that based on the adoption of Risk Management. In addition to this principle, Article 25 of the GDPR adds the requirement to implement Data Protection By Design. This was previously known as Privacy By Design.

The aim of Privacy by Design is to ensure that data protection is included as a consideration and a risk assessment carried out, at the design phase, when determining the means of the processing of any personal data. For proposed changes to systems and processes, data protection must be taken into account at this initial, design stage. This means that all new implementations should take this into account at the very earliest stages (initiation). It is really all about in incorporating data protection risk assessment into change management.

There are also specific security obligations under Article 32, Security of Processing. There is a requirement to adopt appropriate technical and organisational measures to ensure an appropriate level of security of both the processing and the processing environment. This means that what is considered good security practice is mandated as a legal minimum

Cyber Threat Significance

Former US President Obama declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America’s economic prosperity in the 21st century will depend on cyber security.”

Cyber Security Definition

One of the six (or seven - if you include Accountability) GDPR principles that has been at the forefront of all data protection, is that of security. It was also one of the Eight Principles in the DPA98. This means that you must process personal data securely by using ‘appropriate technical and organisational measures’.

The term *Cyber Security* is a relatively new. The word *cyber* is an abbreviation of the Greek word *cybernetic.* This means *skilled in steering or governing. Security* means *freedom from, or resilience against, potential harm*. Hence the term *Cyber Security* denotes the means by which to prevent harm. In the modern technological context, this means the protection against harm to the systems that are used for the processing of information. .

First and foremost, Cyber Security is a form of protection against threats to electronic equipment used by organisations and individuals. It is a defence against malicious attacks on hardware such as; computers, servers, mobile devices, electronic systems, and networks. It also includes protection for software and data processed and stored on associated hardware.

Cyber Security for Small Business

Cyber Security deploys technologies, processes and controls to protect against malicious (external) attacks as well as utilising training, education, awareness, and producing adequate policies and procedures. The aim of cyber security is to reduce the risk of any cyber-attacks. Accreditation in terms of International standards such as ***ISO 27001*** for Risk Management and ***Cyber Essentials*** - an accreditation. scheme within the UK, will not only provide evidence of compliance but will prove to be a great advantage in winning business. Indeed, in the near future this will be stipulated requirement in contracts.

ISO 27001 is a specification for an ISMS that is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

Cyber Essentials is implemented to guard against the most common cyber threats and demonstrate your commitment to cyber security through a formal independent assessment and accreditation.

In order to be confident that you are complying with the requirements of GDPR, PECR (rules for Direct Marketing and personal data - see my ebook on Direct Marketing) and Cyber Security, there are a number of steps that can be taken. The first is to adopt the understanding that compliance has two halves; the rules and the operations against which those are set against.

Help in understanding the rules can be outsourced to an expert or training acquired. In terms of operational activity, having an effective and efficient information management regime is crucial. It also provides business benefits in terms of reduced costs and better processing, storage and dissemination mechanisms.

Risk Assessment

Cyber risk assessments are defined by NIST as risk assessments are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.

Risk is the likelihood of reputational or financial loss It may be measured from zero, low, medium, to high. There are three factors that feed into a risk vulnerability assessment. These are: What is the threat? How vulnerable is the system? What is the reputational or financial damage if breached or made unavailable? This gives us an equation to measure Cyber Risk; Cyber Risk = Threat x Vulnerability x Information Value

Risk Assessment is fundamental to managing Cyber Security. Undertaking a Risk Assessment will help you to ensure that the cyber security controls put in place are appropriate and so allow you to best utilise time, effort and resources accordingly.

There are two complementary techniques that may be utilised to look at risk. They address the problem from different aspects. One is that of the Component-driven risk management approach that focuses on the technical components. This analyses the threats and vulnerabilities faced. A System-driven risk approach comes from the opposite angle and analyses systems as a whole.

The main risks can be categorised as set against the three essential components of information security that reflect the safe utilisation, flow, and storage of information.

These risks are; Confidentiality, Integrity and Availability. These CIA principles can be compromised as follows;

Confidentiality – ensuring that information held is not disclosed or made available to anyone who should not have access to it through unauthorised access to and/or harvesting of information;

Integrity - ensuing that the information held is accurate and can only be accessed and maintained by authorised staff and not subject to unauthorised alteration and/or manipulation; and,

Availability – Ensuring that the information held is available when required and by whatever means that are authorised and not subject to any potential loss and/or disruption to, the availability of information and systems used.

There are also an additional two components that are now regarded as important. These are;

Authentication - The identification of those with authorisation on to the systems prior to being allowed to access the information.

Non Repudiation

Providing details of who has done what and when so that the transaction cannot be repudiated.

Cyber Threats

If you want to hit a country severely you hit its power and water supplies. Cyber technology can do this without shooting s single bullet

- Isaac Ben-Israel, Major General - Israeli Air Force

A Cyber Threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.

There is a very significant risk to data from a cyber-attack. This may take place at all levels – organisational or national. The nature of cyber threats is constantly evolving in terms of both sophistication and volume of attacks.

Cyber Threats emanate form a number of sources. these are;

- Hackers:
- Hacktivists:
- Disgruntled insiders:
- Accidental actions of authorized users:
- Natural disasters;
- Other - Hostile nation-states, Terrorist groups, Corporate spies and organised crime

The threat of Cyber Attacks is what derives the need for Cyber Defence. If there were no crime finals, you wouldn't need any police!

Types of Cyber Attacks

- **Advanced persistent threats arise** when an unauthorised user gains access to a system or network and remains without being detected for an extended period of time.
- **Data Destruction** occurs when a cyber attacker attempts to delete your data
- **Data manipulation** aims to change the data to make it harder for an organisation to operate.
- **Distributed denial of service (DDoS) attacks** look to disrupt a computer network by flooding the network with superfluous requests in order to overload the system and prevent legitimate requests being fulfilled
- **Drive-by downloads** happens without a person's knowledge often installing a computer virus, spyware or malware
- **Intellectual Property Theft** is stealing or using someone else's intellectual property without permission to gain a commercial advantage.
- **Malvertising** is the use of online advertising to spread malware.
- **Malware (Malicious Software)** is software that performs malicious tasks on a device or network such as corrupting data or taking control of a system.
- **Man-in-the-middle attack (MITM attack)** is when an attack relays and possibly alters the communication between two parties who believe they are communicating with each other
- **Phishing attacks** is when a cybercriminal attempts to lure individuals into providing sensitive data such as personally identifiable information (PII), banking and credit card details and passwords.
- **Ransomware** is a type of malware that denies access to a computer system or data until a ransom is paid.
- **Rogue software** is malware that is disguised as real software.
- **Spyware** is a form of malware that hides on a device providing real-time information sharing to its host, enabling them to steal data like bank details and passwords.

- **Trojan** creates a backdoor in your system, allowing the attacker to gain control of your computer or access confidential information
- **Unpatched software**Unpatched software is software that has a known security weakness that has been fixed in a later release but not yet updated.
- **Wiper attack** is a form of malware whose intention is to wipe the hard drive of the computer it infects
- **Zero-day exploits are** flaws in software, hardware or firmware that is unknown to the party or parties responsible for patching the flaw. This is why software testing is vital, albeit that it may not immediately uncover all problems.

Please note that while Cyber Attacks are usually thought of was emanating externally - from outside of the organisation, you cannot ignore the internal threat from employees who may be disgruntled and wish to cause harm. Not forgetting the Social Engineering attacks, where a lack of awareness amongst employees may result in vulnerabilities that are exploited.

Cyber Vulnerabilities

A Vulnerability refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

They also include Social Engineering – human behaviour that can be exploited such as entering buildings by tailgating and thereby accessing information, providing information inadvertently through email and telephone calls.

Cyber Defence – In Context

In order to reduce the risk of a breach from a Cyber attack, an effective Cyber Security regime needs to be in place. This requires a strategic and proactive approach, affecting all areas of the organisation. It needs to fall in line with the overall business strategy. It also needs to take into account not just the technical aspect (technology), but the equally important people and process elements as well. Effective Cyber Security requires a risk management approach, bought into by senior management, together with the implementation of adequate controls.

Cyber Defence - Basics

The model of activity has a virtuous cycle of inter-related activities.

These are;

- Creating policies and procedures,
- Dissemination to staff through communications, awareness and training,
- Monitoring and undertaking audits to ensure compliance (proactive),
- Breach reporting to investigate what has gone wrong and;New item
- Rectification by means for re-assessment of each component activity. All the while, refining the Risk Assessments.

Cyber Defence - Delivery

Invoking a secure Cyber security regime consists of the following activities;

- Adoption of best practice from whichever source (policies, procedures, governance etc.)
- A Risk Management based approach of assessing risk and agreeing resources
- An implementation phase followed by a consolidation with the implementation of full
- Operational day to day Cyber Security governance
- Installation of Cyber Defences; Anti-Virus, Firewalls etc.
- Penetration Testing undertaken
- Accreditation for Cyber Essentials as a first major deliverable to measure technical
- Cyber Essentials Plus and possibly ISO27001 later
- Ongoing engagement with other associated activities and functions;
- Data Protection activities to ensure Information Asset Registers and Records Retention are up to date
- Ongoing communications, awareness and training for all staff
- Access to expertise and membership of knowledge groups
- Disaster Recovery and Business Continuity Management

Cyber Security deploys technologies, processes and controls to protect against malicious (external) attacks. The aim of cyber security is to reduce the risk of any cyber-attacks.

Accreditation

Fortunately, there are existing standards that are available to establish the assurance that Cyber Security is operating as it should. Two of the common ones are: Cyber Essentials and ISO 27001. The Cyber Essentials scheme is an assurance mechanism, independently assessed at affordable costs for organisations – (around £300) of all sizes. It provides evidence to patients, regulators and other stakeholders that the most important cyber security controls have been implemented.

The scheme provides five security controls. The UK government has asserted that implementation of Cyber Essentials could prevent “around 80% of cyber-attacks”. ISO 27001 (formally known as ISO/IEC 27001:2005) is a tried and tested specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

Adoption of an ISO 27001 ISMS will ensure every aspect of Cyber Security is addressed. Implementing ISO 27001 and Cyber Essentials provides evidence from an independent assessment that standards are being applied.

Benefits of Accreditation

Provides evidence to the ICO of a level of compliance Informs your customers of the level of security applied to their data Sets a baseline level of standards and controls that can be adopted as day to day procedures Can help you win customers – most will require some evidence of compliance From 1 October 2014, the government required all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

Provides evidence to the ICO of a level of compliance Informs your customers of the level of security applied to their data Sets a baseline level of standards and controls that can be adopted as day to day procedures] Can help you win customers – most will require some evidence of compliance

Cyber Security Incident - 5 Phases

Planning for a Cyber Incident

It is vitally important to understand the implications of a Cyber Attack and the implications that arise from one.

Having Disaster Recovery and Business Continuity Plans in place is needed for all circumstances - even if the problem is not caused by a Cyber Attack - e.g. floods, theft, pandemics (topical) etc.

There are 5 stages to preparation;

Plan and Prepare:

In advance

Detection and Reporting:

Reporting of “events” that might be or turn into incidents;

Assessment and decision:

Undertake an assessment of the situation to determine whether it is in fact an incident;

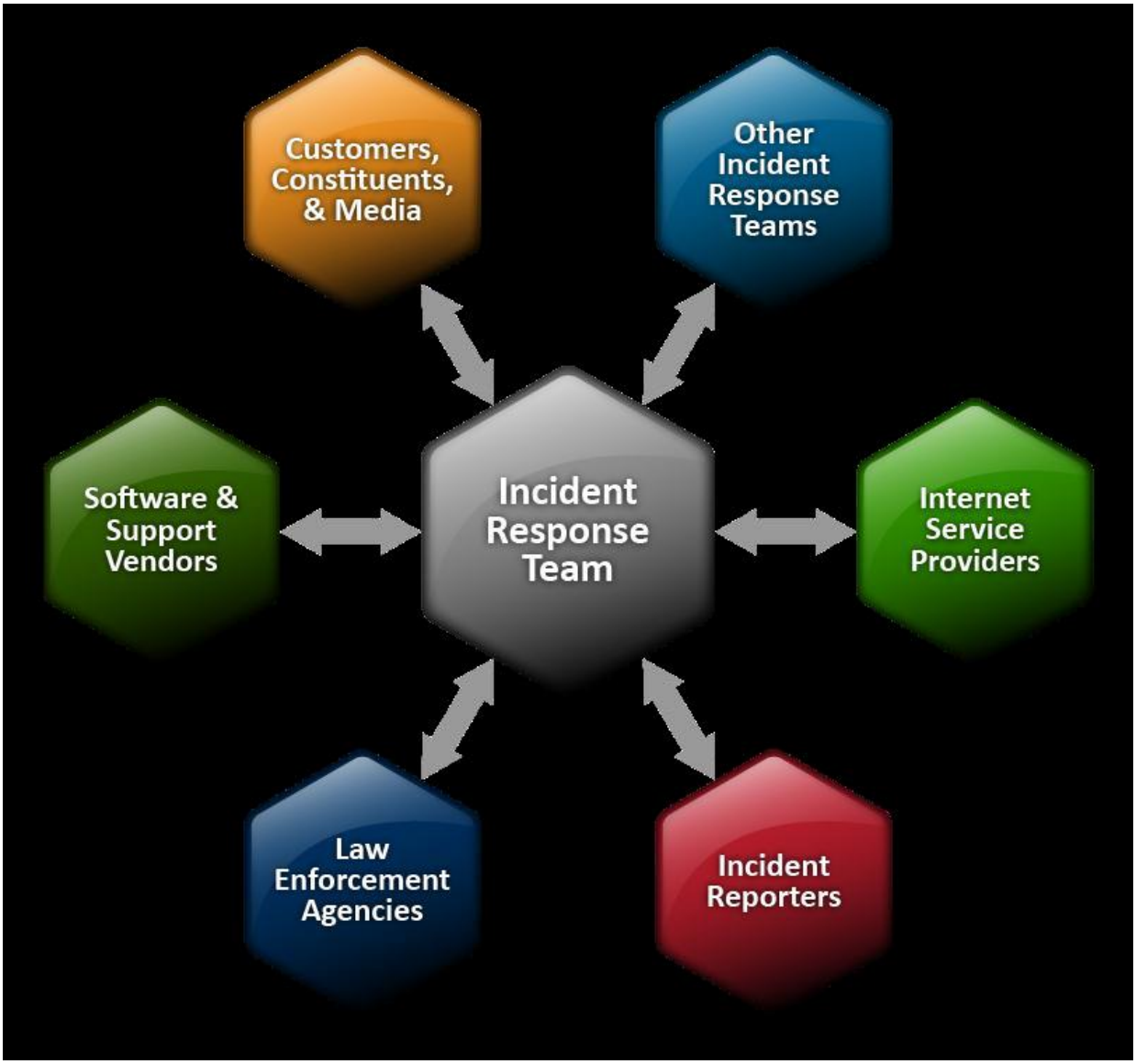
Responses – Disaster Recovery: containment, eradication, recover from and forensic analysis of the incident, where appropriate;

Review-

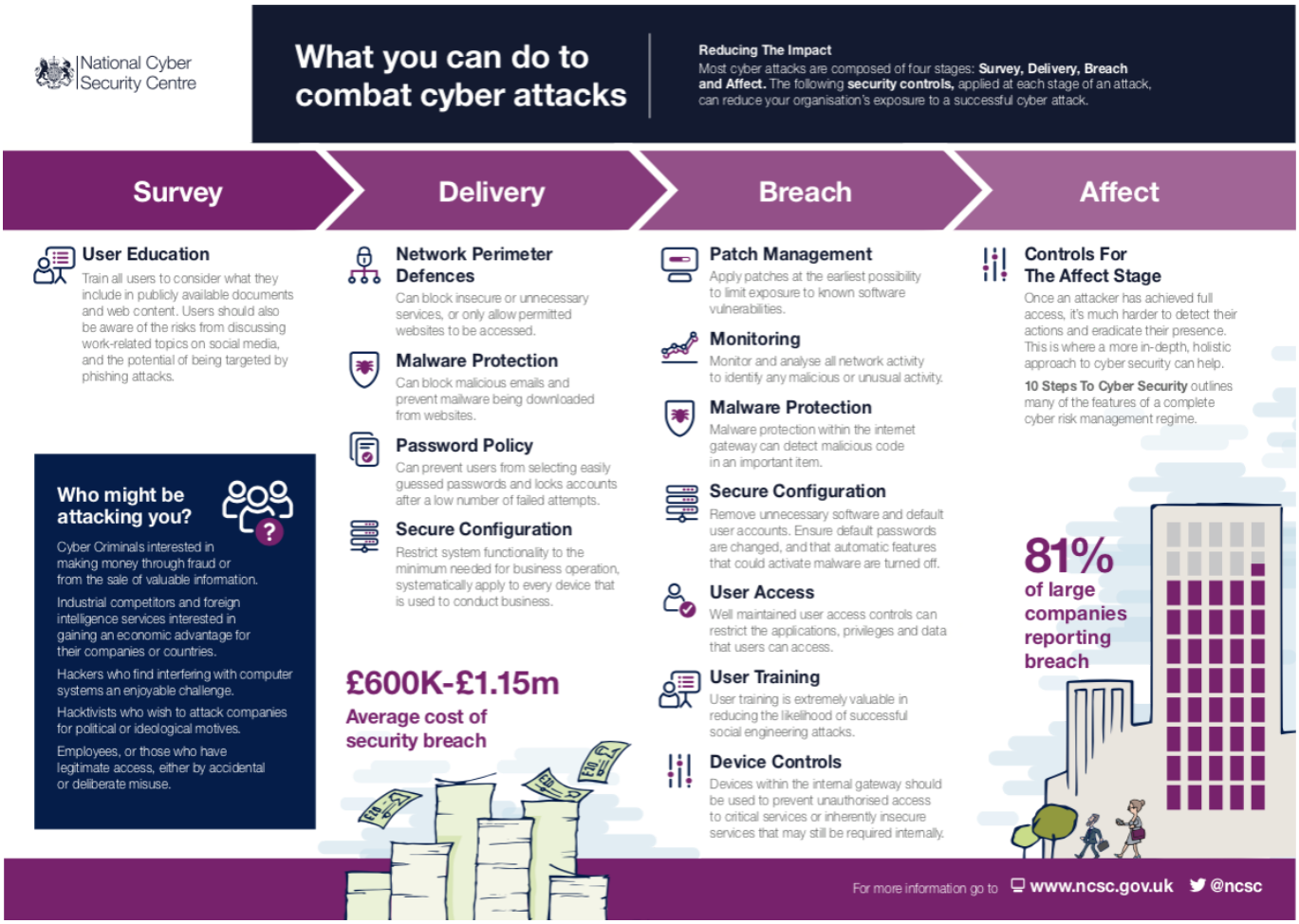
Lessons learned: Improving the management of information risks as a consequence of incidents experienced.

Managing Cyber Incidents


1
Identify
AM: Asset Management
BE: Business Environment
GV: Governance
RA: Risk Assessment
RM: Risk Management Strategy
2
Protect
AC: Access Control
AT: Awareness Training
DS: Data Security
IP: Information Protection Processes and Procedures
PT: Protective Technology
3
Detect
AE: Anomolies and Events
CM: Security Continuous Monitoring
DP: Detection Processes
4
Respond
RP: Response Planning
CO: Communications
AN: Analysis
MI: Mitigation
IM: Improvements
5
Recover
RP: Recovery Planning
IM: Improvements
CO: Communications
NIST Cyber Security Framework



NIST Cyber Incident Response Diagram



Cyber Attacks and how to respond - National Cyber Security Centre information

The Author - Thomas Hayes

Thomas Hayes has more than 30 years practical experience in; business analysis, project management, Information Management & Governance, Data Protection as well as business up to Managing Director level, managing large business change and transformation.

He has provided consultancy services within many private and public sectors within. Europe, USA and China.

He has the following formal qualifications; • BA Honours in Politics & Contemporary History • Part-qualified Accountant ACMA Professional Part 2 • Association for Project Management qualified • Certificate in Information Governance for Health & Social Care • Fellow of the British Computer Society • BCS Chartered IT Practitioner • GDPR Foundation & Practitioner Certificate • IAPP Fellow, CIPP/E, CIPM • BCS CISMP • Certified Cyber Security Practitioner pending • Advanced Diplomas in Stress Management, NLP, Life Coaching, TEFL and Advanced TEFL• Published Author

.

Website; **www.hayesltd.com**

Email: **thayes@hayesltd.com**

Contact Telephone: **07834 039328**