



Haines Watts

Cyber Security for Businesses:
Safeguarding Your Digital Assets

Contents

Page 4 – Introduction

Page 5 – Chapter 1: Understanding Cyber Threats

Page 7 – Chapter 2: Assessing Your Digital Vulnerabilities

Page 8 – Chapter 3: Developing a Robust Security Strategy

Page 10 – Chapter 4: Implementing Secure Network Infrastructure

Page 12 – Chapter 5: Protecting Data Privacy and Confidentiality

Page 13 – Chapter 6: Preventing Social Engineering Attacks

Page 14 – Chapter 7: Responding to Cybersecurity Incidents

Page 15 – Chapter 8: Building a Culture of Cybersecurity Awareness

About the Author

Matthew Wilkinson-Foster

ISC2 Certified in Cybersecurity, Microsoft Certified Professional

With over 20 years of experience in IT, Matthew is an expert in advising business owners on all aspects of technology. Throughout his career, he has successfully led IT infrastructure design, IT security and cloud migration programs for businesses of all sizes. He understands the unique challenges businesses face in today's constantly changing IT landscape. Through his extensive experience, Matthew recognises that there is no one-size-fits-all solution in IT, and has honed his skills in virtualization technologies, IT security, cloud hosting, and system migrations to best serve his clients.

Email: it.wolves@hwca.com

Telephone: 01902 793333

Introduction

In today's interconnected world, businesses of all sizes face a significant challenge: protecting their digital assets from cyber threats. The advancement of technology has provided countless opportunities for organizations to thrive, but it has also exposed them to new risks. Cybercriminals are constantly evolving their tactics, using new and innovative technologies like AI, targeting businesses to exploit vulnerabilities and steal sensitive data. To ensure the long-term success and sustainability of your organization, it is crucial to prioritise cyber security.

"Cyber Security for Businesses: Safeguarding Your Digital Assets" is a guide that aims to equip business owners and executives with the knowledge and tools necessary to establish a strong defence against cyber threats.

This eBook will provide actionable insights and practical strategies to mitigate risks, protect sensitive information, and build a resilient cyber security posture.

Chapter 1: Understanding Cyber Threats

In this chapter, we delve into the world of cyber threats, exploring the different types of attacks that businesses may face. We discuss the motivations behind cybercrime, such as financial gain and activism. By understanding the adversary's mindset, you can better prepare yourself to defend against their tactics. We also highlight notable cyber-attacks that have affected businesses in recent years, showcasing the potential consequences of inadequate security measures. This chapter serves as a foundation for the subsequent chapters, laying the groundwork for a comprehensive understanding of cyber security.

Common types of cyber threats:

Malware – Malicious Software (Malware) is a file or code that infects, explores, steals or conducts virtually any behaviour an attacker wants.

Ransomware – A type of malware designed to deny a user or organization access to files on their computer, encrypting all files and demanding a ransom payment for the decryption key.

Phishing – A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the cybercriminal purports to be a legitimate person or business.

DDoS attacks – A Distributed Denial-of-Service (DDoS) attack is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and websites.

Identity-Based Attacks – Identity-based attacks occur when cybercriminals target your computer system, network, or account to retrieve your personal information for illegal or malicious activities. Also known as impersonation attacks.

Insider Threats – An insider threat is a threat where an employee or a contractor will use his or her authorized access, knowingly or unknowingly, to do harm to the security and data of the company.

Motivations behind cybercrime:

Financial gain – This is the most common reason for a cyber-attack. Cybercrime gangs will gain access to a company's IT systems to steal sensitive and personal data to sell it on to the highest bidder.

Intellectual property theft – Stealing an idea, creative expression, or invention from an individual or a company. IP theft can refer to someone stealing patents, copyrights, trademarks, or trade secrets. This type of theft is often committed to hold a company or individual to ransom.

Political activism – A cybercrime gang or hacker will attack the IT systems of political parties to leak information or use as blackmail in an attempt to bring political or social change.

Notable cyber-attacks (at the time of writing):

WannaCry – 2017 – NHS suffers biggest attack to date

RockYou2021 – 2021 – Largest password compilation of all time leaked online with 8.4 billion passwords

Twitter – 2022 – Flaw in Twitter platform helps leak 5.4 million user account details in a Social Engineering Attack

MOVEit data breach – 2023 – A cyber-attack which targeted the MOVEit file transfer system exposing very sensitive employee data from high-profile businesses

Chapter 2: Assessing Your Digital Vulnerabilities

Before implementing any security measures, it is essential to identify and assess your organisation's digital vulnerabilities. This chapter guides you through the process of conducting a thorough assessment, including vulnerability scanning, penetration testing, and risk analysis. By evaluating your system's weaknesses, you can prioritise and address the most critical areas.

Conducting vulnerability scans – Conducting a vulnerability scan on your internal systems is the first step in establishing a base line for your IT. A vulnerability scan helps you understand the current state of your IT and helps in developing a strategy for improvement.

Performing penetration testing – Penetration tests are performed to identify weaknesses in network security both internally and from the outside world. A penetration test (or Pentest) gives you real idea of what your public exposure looks like and how easy it would be for a “bad actor” (Hacker) to breach your security measures.

Risk analysis and prioritisation of vulnerabilities based on potential impact – After conducting a vulnerability scan and performing a Pentest, you are now in a position where you can see how vulnerable your IT systems are. The next step is to assess the risks and analyse the result by prioritising them based on the potential impact to the business. By creating a remediation list based on risk and impact, you are giving your business and your IT systems the best chance of surviving an attack, as long as the remediation work is carried out swiftly upon discovery.

The longer these vulnerabilities exist, there is more chance of them being exploited.

Regular testing of your IT environment is key to staying on top of any new vulnerabilities.

Chapter 3: Developing a Robust Security Strategy

Building a robust security strategy is a fundamental step towards safeguarding your digital assets. In this chapter, we explore the key elements of a comprehensive security strategy, including policy development, risk management, and incident response planning. By creating a well-defined security strategy, you can effectively allocate resources and establish a proactive defence against cyber threats.

Creating a comprehensive security policy that outlines acceptable use and security protocols – One of the main reasons for creating a comprehensive security policy is so that everyone knows what is and is not acceptable when using an organisation's IT systems and more importantly what to do if a user suspects that they or someone else has observed suspicious activity.

Implementing risk management frameworks – Risk management frameworks are a good way to keep your IT systems in check. There are several risk management frameworks like ISO 27001 or NIST Cybersecurity Framework. However, a good place for all businesses to start is with the UK government backed Cyber Essentials Cybersecurity risk management process for identifying risks.

Developing an incident response plan with clearly defined roles and responsibilities – So, a user has reported that they have noticed strange activity on some files on your network. What do you do??

Well, this is where you need to have a clear incident response plan that sets out who is responsible for the implementation of the plan and the roles others play in the investigation and remediation of the incident. An incident response plan should include logs of what happened and what has been done at every stage. This will then make it easier to explain to the Independent Commissions Office what happened if you suffer a breach.

****Remember – You have 72 hours from first noticing a breach to investigate it and report it to the ICO if necessary.***

Chapter 4: Implementing Secure Network Infrastructure

A secure network infrastructure is the backbone of a resilient cyber security framework. This chapter focuses on the essential components of network security, such as firewalls, intrusion detection systems, and secure remote access. We delve into strong authentication mechanisms and encryption protocols. By implementing robust network security measures, you can fortify your organisation's perimeter defences and minimise the risk of unauthorised access.

Configure firewalls to filter traffic – Configuring your firewall to block incoming and outgoing network traffic allows you to control what is allowed in and out of your network and to which web services. Firewalls are rule based devices. To allow traffic in and out there must be a rule to allow the action. For example, if you had a webserver in your office for public access you would have a rule similar to “Allow all traffic to the webserver”. This rule will allow the outside world into the office webserver. The same is true of outgoing rules. You may have an outgoing rule that looks similar to “deny access to www.facebook.com”. Outgoing rules aid in the prevention of employees accessing something that could compromise your network. Many businesses overlook outbound rules through fear of upsetting employees because they are not allowed to browse social media on the organisations network, however by allowing access to only the parts of the internet that your employees need to perform their daily duties, you can really cut down the risks of accidentally exposing your business.

Deploy IDS/IPS – Deploying intrusion detection and prevention systems to detect and block malicious activities can stop attackers while they are gathering information about your network. So, what's the difference between IDS and IPS?

Intrusion Prevention Systems (IPS) are there to prevent known security problems from being exploited. An IPS is like a firewall but in reverse. As mentioned above, a firewall has rules like “allow all traffic to webserver”, however an IPS has many, many thousands

of rules such as “block known security flaw xyz...”. The rules in the IPS get updated automatically all the time when a new vulnerability is exposed.

Intrusion Detection Systems (IDS) work in a similar way as IPS. However the IDS will detect if a “bad actor” is trying to exploit a vulnerability by “sniffing” the incoming internet traffic and blocking it.

VPNs, SSL and MFA – Establishing secure remote access through the use of virtual private networks (VPNs), Secure Socket Layer protocol (SSL) and Multi-Factor Authentication (MFA) is good, but what are they?

VPN or Virtual Private Network is a network connection that creates a private link over the internet between two points, for example the office and your house. Using this link, you have direct access from you house to the office network and all the data is being encrypted so that the data cannot be read by a third party while it is being sent between the two locations.

SSL or Secure Socket Layer is a protocol for securing data transmission between two devices by using encryption. A real-world example of this is that on the majority of websites you will notice a little padlock in the left-hand side of the address bar. This little padlock means that any information that is sent between your computer and the website is encrypted and generally speaking more secure.

**** Due to the ease of obtaining an SSL certificate don't assume all websites are safe just because they have the little padlock. You should always use some common sense ****

MFA or Multi-Factor Authentication is a way of making sure the login details are being used by the correct individual and not by a hacker that has stolen the details. MFA requires users to provide two or more verification factors to gain access to a website, application, or corporate network.

Chapter 5: Protecting Data Privacy and Confidentiality

Data privacy and confidentiality are paramount concerns for businesses, particularly with the introduction of data protection regulations. In this chapter, we explore strategies for protecting sensitive data, including encryption, access controls, and data classification. By prioritising data privacy and confidentiality, you can build trust with your customers and stakeholders while mitigating the risk of reputational damage.

Encrypting your data – Implementing encryption algorithms like AES or RSA to protect sensitive data can help mitigate against the loss or theft of devices, but data encryption doesn't stop there. In an ideal world, data should be encrypted in its three states – at rest (data backups, data on your computer or devices), in use (data being used by applications or employees) and in transit (data being sent somewhere – e.g. file exchange). By implementing security measures to make sure your data is encrypted in all three states you will help keep your data safe.

Controls and Permissions – Applying access controls and user permissions to limit data access is the best way to make sure sensitive data is only seen by those who need to see it.

Classify your data – Classifying data based on its sensitivity and implementing appropriate protection measures ensures that you know where, what and how much sensitive data you have and need to protect.

Business impact – The potential impact on any business following a cyber-attack could be catastrophic. Not only could there be a financial impact from paying fines and in some cases the ransom (although I wouldn't condone paying the ransom, always have backups!) but there is also the reputational damage that can occur. While the financial impact can be dealt with instantly, the reputational damage will last much longer and can often be the cause of a business failing following a breach if the financial cost doesn't cause the business to fail first.

Chapter 6: Preventing Social Engineering Attacks

Social engineering attacks continue to be a prevalent threat vector, exploiting human vulnerabilities to gain unauthorised access to systems and sensitive information. In this chapter, we examine forms of social engineering, such as phishing. By fostering a culture of security awareness, you can effectively combat social engineering threats.

Educating employees – Educating employees about common social engineering techniques and how to spot them is a key step in mitigating these types of attack. If you arm your employees with the necessary information the chances of suffering a social engineering attack are dramatically reduced.

Filter your emails – Implementing email filters to detect and block phishing attempts is a basic need in the fight against common attacks. Don't just assume that your email is being filtered by your provider, reputable email filtering services will cost money, but this is nothing in comparison to what the financial damage could be if you don't have email filtering implemented.

Simulate phishing attacks – Conducting simulated phishing campaigns will give your business an insight into the knowledge of your employees when it comes to cyber security. Once you have simulated an attack you can use the results to raise awareness and reinforce the training your employees have received.

Chapter 7: Responding to Cybersecurity Incidents

Despite all preventive measures, cybersecurity incidents may still occur. This chapter focuses on the importance of a well-defined incident response plan. We discuss the key elements of the role of incident response teams, communication protocols, and post-incident analysis. By having a robust incident response plan in place, you can minimise the impact of cyber-attacks and ensure a swift recovery.

Developing an incident response team

Developing an incident response team and defining their roles and responsibilities is a necessity of any incidence response. An incident response team can oversee the response process by helping to identify how and why the response is needed. The incident response team is also there to make sure all communications happen when they are supposed to.

Establishing communication channels

Establishing communication channels and protocols for reporting and handling incidents helps with the containment of the incident by communicating with the people, organisations and governance authorities. Clear channels of communication are essential to get the information out in a swift and concise manner.

Conducting post-incident

Conducting post-incident analysis enables the business to identify areas for improvement and prevent future incidents. Any business needs to understand how the data breach happened in order to mitigate a future incident.

Chapter 8: Building a Culture of Cybersecurity Awareness

Cybersecurity is not solely the responsibility of the IT department; it requires the participation and commitment of every individual within an organisation. In this final chapter, we discuss strategies for fostering a culture of cybersecurity awareness throughout your business. We provide guidance on employee training programs, security awareness campaigns, and the establishment of security policies. By empowering your workforce with the knowledge and skills to identify and mitigate risks, you can create a collective defence against cyber threats.

To foster a culture of Cybersecurity awareness in your business, you need a two-pronged approach. The first prong starts at the top with the stakeholders, business owners and board members. You need full management commitment not only to learn about the benefits of fostering a Cybersecurity awareness culture within the business but to also adhere to it and lead from the front. This is often the hardest part.

The second part or prong is to work from the ground up. The most vulnerable part of any IT system is the part that involves a human. This may sound a little harsh, but it is true. The majority of cyber incidents are due to a member of staff clicking on something they should not have; be it a link in an email, ignoring a web browser attempt to stop them by clicking “continue to the site anyway” or by being in too much of a rush to stop and think “Is this request genuine and why would they ask me to do that?”

By providing staff training, you raise awareness of the Cybersecurity risks and make sure all staff have the tools they need keep your business protected.

Providing regular cybersecurity training and awareness programs for employees

Not many businesses realise that when it comes to IT security, employees need two levels of training.

- 1) **Security Awareness** – Security awareness training raises the awareness of security within your organisation's specific operational environment. This training is crucial to help employees identify insider threats and to identify when an attacker is trying to compromise data.
- 2) **Cybersecurity Training** – By providing dedicated Cybersecurity training you keep your employees up to date with the latest types of threat; for example, how not to get pulled into the latest phishing email or vishing attempt.

Encouraging reporting of security incidents and rewarding proactive security behaviours

Encouraging and rewarding your employees for reporting security incidents is a great way for employees to feel engaged with the cybersecurity of the business. The rewarding of positive behaviours has multiple benefits – one of the benefits is that your employees will feel valued in what they do and are subsequently more productive. Another benefit is that when an employee feels comfortable to report potential security incidents, these incidents can often be contained or in some cases completely mitigated. Encouraging and rewarding your employees doesn't need to be an expensive gesture, of course, every employee would like new car for their efforts; however, this approach could also have the opposite effect.

In simple terms – employees like to feel valued. So next time an employee raises a question about a file changing or a potentially malicious email, just remember to say, "Thanks for highlighting that". Ultimately your employees are the ones who will be adhering to the IT security policy. If the policy is scary and instils fear into your employees, it will have the opposite effect to what you intended as employees will not engage and you will be none the wiser regarding breaches of data.

Incorporating Cybersecurity into the organisation's values

Incorporating Cybersecurity into the organisation's values shows that your organisation is serious about its Cybersecurity from both an internal standpoint, which will show your employees that the data they hold is worth protecting, and externally you will show clients that you value their data and will do your utmost to protect it.

At Haines Watts Wolverhampton we can help you achieve the IT security you need to protect your business. We provide practical advice on aligning your security objectives with your business goals and developing a roadmap for implementation.

For further information email – it.wolves@hwca.com

Each chapter in "Cyber Security for Businesses: Safeguarding Your Digital Assets" offers valuable insights to enhance your organization's cyber security posture. By implementing the concepts outlined in this book, you can protect your digital assets, maintain customer trust, and ensure the long-term success of your business in an increasingly interconnected world.

Author: Matthew Wilkinson-Foster
Cover photo: Luis Villasmil