STEADFAST SOLUTIONS

THE 7 LAYERS OF CYBER SECURITY

TABLE OF CONTENTS

01 CHAPTER 1: INTRODUCTION

While it's now easier to connect, communicate, and collaborate, it's also become increasingly essential to safeguard our virtual lives. Digital footprints are not limited to social media profiles – they encompass personal information, business data, financial details, everything. This invaluable data attracts a new breed of criminals — cyber-attackers. They exploit vulnerabilities in systems, networks, and even human behaviour to gain unauthorised access, steal, and sometimes hold information hostage.

Cyber threats aren't confined to big corporations or government entities. Everyone, from the individual browsing the internet at home to a multinational company, is at risk.

In essence, cyber security can’t be an afterthought anymore; it’s a necessity. Just as we lock our homes before leaving or put on seatbelts while driving, ensuring our digital safety needs to become second nature.

It's a common misconception that cyber security is just about having a strong password or installing the latest antivirus software. While these are vital components, there's so much more to the story. Cyber security is like the layers of an onion. Peel back one layer, and there's another underneath.

The seven layers of cyber security work in tandem to create a resilient shield, protecting personal data, intellectual property, critical infrastructure, and everything in between.

02 CHAPTER 2: THE HUMAN FACTOR: YOUR FIRST LINE OF DEFENCE

At the heart of many cyber incidents, you'll often find a human error. It's not that people are inherently careless, but without proper guidance, mistakes can happen.

Here are some of the most common slip-ups:

- **Weak passwords:** Using passwords like “password” or “12345” might seem convenient, but they are also easily guessable. Cybercriminals often use tools that can attempt thousands of words a minute, making weak passwords a prime target.
- **Clicking on unknown links:** A curious click on a seemingly innocent link can inadvertently download malware or lead to phishing sites designed to steal information.
- **Sharing sensitive information:** Be it on social media, an innocuous email, or even just lending someone your mobile phone, sharing too much can give malicious actors a gateway into your systems.

Threat actors fully take advantage of people’s trusting natures through one of the most common types of cyber-attacks: social engineering. This involves exploiting human psychology; for example, a threat actor might impersonate a colleague over the phone, or craft a convincing fake email from a trusted organisation to manipulate people into divulging confidential information or performing specific actions.

What makes this threat particularly insidious is their reliance on human emotions, like trust and curiosity. It reminds us that cybercriminals aren't always faceless codes; sometimes, they're individuals adept at understanding and manipulating human behaviour.

Recognising the human factor's importance in cyber security leads to a clear solution: education and awareness. By empowering individuals with knowledge, you can transform potential vulnerabilities into strengths.

- **Regular training sessions:** Many managed service providers (MSPs) provide cyber awareness training. This is usually delivered through video-based content, interactive online sessions, quizzes, recent cyber security news, and other training modules.
- **Phishing simulations:** In a controlled environment, simulated phishing emails can be sent to gauge how individuals react. It provides a practical learning experience and highlights areas for improvement.
- **Creating a culture of cyber awareness:** Encouraging an environment where people can report mistakes or suspicious activities without fear of reprimand ensures that potential threats are addressed swiftly.

As we delve deeper into the layers of cyber security in the upcoming chapters, it's essential to remember the human factor's pivotal role. Harnessing human potential and awareness can make the difference between a secure environment and one riddled with vulnerabilities.

03 CHAPTER 3: PERIMETER SECURITY: YOUR DIGITAL MOAT

The perimeter represents the boundary between an organisation's internal network and the vast expanse of the internet. An unsecured digital perimeter exposes systems, data, and applications to a myriad of cyber threats. Intruders could potentially eavesdrop on communications, steal sensitive information, or launch disruptive attacks.

- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS):** These attacks aim to overwhelm network resources, causing disruptions or complete shutdowns. DDoS attacks amplify this by utilising multiple sources to flood the target.
- **Zero-day exploits:** These are attacks on software vulnerabilities unknown to the vendor, meaning there's no fix available at the time of the attack.
- **Port scanning:** This is the digital equivalent of a thief checking for unlocked doors. Attackers probe network ports to find potential entry points.

The perimeter, as our initial defence line, is essential in the layered approach to cyber security, safeguarding an organisation's internal networks, systems, and data from unauthorised access.

- **Firewalls:** The primary gatekeepers, firewalls filter incoming and outgoing traffic based on predefined security policies. While basic firewalls block traffic based on IP addresses and ports, modern, next-generation firewalls dive deeper, inspecting packet contents and even understanding application behaviours.
- **Intrusion Detection and Prevention Systems (IDPS):** IDPS solutions continuously monitor network traffic. When they detect suspicious activities or known malicious patterns, they trigger alerts. Prevention systems take it a step further, not just detecting but also blocking the malicious traffic.
- **Virtual Private Networks (VPNs):** VPNs create a secure, encrypted tunnel for data transmission between the user and the network, ensuring that even if data is intercepted, it remains unreadable.

Cisco, for example, is a leading IDPS solution, operating in the cloud to provide broad, agile security coverage. It utilises threat intelligence, machine learning (ML), and artificial intelligence (AI) to identify emerging threats, detecting and blocking malicious activities even before they become widespread.

With threats becoming increasingly sophisticated and pervasive, a robust perimeter security ensures that potential attackers are deterred, detected, or deflected right at the boundary, long before they can infiltrate deeper into the network's core.

04 CHAPTER 4: NETWORK SECURITY: NAVIGATING THE VEINS OF YOUR DIGITAL WORLD

Your network is like a circulatory system – data packets travel through this intricate web, much like blood cells rushing through veins, to facilitate communication, collaboration, and data exchange. But, like any system, it's susceptible to various ailments and threats.

- **Distributed Denial of Service (DDoS):** As mentioned in Chapter 3, attackers use DDoS to inundate a network with excessive traffic, rendering it inaccessible to legitimate users.
- **Man in the Middle (MITM):** Threat actors are able to intercept communication between two parties without their knowledge, eavesdropping, manipulating, or even stealing the information being exchanged.

Network security is designed to protect the integrity, confidentiality, and accessibility of data as it moves across the network. A broad variety of tools, practices, and solutions can be used to design a secure network and build another layer of strong cyber security.

- **User access controls:** Implementing user access controls, such as the principle of least privilege or zero-trust architecture, reduces potential attack vectors and provides greater visibility across your network.
- **Regular audits:** Periodic checks ensure the network's health and security, identifying vulnerabilities and rectifying them proactively.
- **Encryption:** By converting data into a code, encryption ensures that even if a malicious actor intercepts it, the information remains unreadable without the decryption key.
- **Antivirus and antimalware:** These software solutions continuously scan the network for malicious entities like viruses, ransomware, or spyware, neutralising them before they can wreak havoc.

A more advanced, sophisticated measure of network security can be found in Security Information and Event Management (SIEM) solutions. Through intelligent security analytics, threat detection, and proactive threat hunting, these tools offer a centralised view and aid in detecting, monitoring, and analysing anomalous activities across the network. Microsoft Sentinel SIEM is a prime example, leveraging Microsoft's AI and ML capabilities to detect unusual and potentially harmful patterns, and assisting security teams in quickly identifying and mitigating threats.

With the increasing interconnectedness of systems, a singular vulnerability or breach can have a cascading effect, compromising an entire ecosystem. Effective network security not only guards against malicious attacks, but also intercepts inadvertent missteps that could expose sensitive information.

05 CHAPTER 5: ENDPOINT SECURITY: PROTECTING CONNECTED DEVICES

An endpoint is essentially any device that is connected to your network — computers, laptops, mobile phones, tablets, and even smart devices. They act as gateways, or access points, into your network, and just as you would ensure every door and window to your house is locked, so must you take precautions to ensure the endpoints connected to your network are fortified against threats.

- **Malware:** A broad term for malicious software, malware aims to infiltrate, damage, or perform unsolicited actions on a device. It encompasses a wide range of threats like viruses, worms, and spyware.
- **Ransomware:** A particularly insidious type of malware, ransomware encrypts a user's data and demands a "ransom" for its release. Victims find their essential files held hostage, often leading to significant financial and data losses.
- **Phishing:** As mentioned in Chapter 2, phishing is generally associated with email, but it can target endpoints. Clicking a deceptive link or downloading a malicious attachment can lead to malware being installed on the device, which in turn, leads threats inside your network.

Protecting endpoints is not just about installing antivirus software and managing patches; it need a holistic approach, from user education to regular maintenance. Protecting user devices will take a certain approach that depends on your business, how your employees work, and many other factors; generally, the following common strategies and tools provide a foundation for an endpoint security strategy to be built on.

- **Device policies:** Many people use their personal laptops or tablets to work these days. A device policy outlining the use of personal PCs and how corporate data is shared will ensure your team is registering every endpoint and not mishandling sensitive information.
- **Mobile Device Management (MDM):** MDM tools can manage, monitor, and secure employees' mobile devices, providing greater transparency and visibility into your employees' workflows and data usage.
- **Regular backups:** Ensuring data is backed up periodically means that if a device is compromised, the data can be recovered without paying ransoms or facing data loss.
- **Multi-Factor Authentication (MFA):** Authentication apps, tokens, or codes means that even if a user's login credentials are stolen, the account will remain locked without the additional authentication.

Given the rise of remote working and the diversification of devices used in modern business environments, ensuring complete endpoint security is imperative. Without it, even one compromised device can serve as a launchpad for broader network intrusions.

CHAPTER 6: APPLICATION SECURITY: BULLETPROOFING APPS

Applications are treasure troves of information, entertainment, communication – they make both our personal and professional lives easier. Unfortunately, this treasure trove is a draw for malicious actors for another reason: apps process, store, and transmit sensitive user information. Beyond mere data theft, compromising an application can provide hackers a foothold, a gateway into broader network systems.

Application attacks are more advanced than mere malware viruses, and are targeted, purposeful actions – which only makes them more insidious.

- **SQL injection:** This occurs when an attacker "injects" malicious SQL code into a query. By doing so, they can view, modify, or delete data in the database, often bypassing application security measures.
- **Cross-Site Scripting (XSS):** In an XSS attack, malicious scripts are injected into websites, which are then executed by unsuspecting users' browsers. This can lead to stolen session cookies, defaced websites, or redirected users to malicious domains.
- **Cross-Site Request Forgery (CSRF):** Here, attackers trick users into performing actions without their knowledge, potentially causing unwanted changes in user settings or data theft.

Ensuring your applications are secure is an ongoing commitment that begins at the development phase – or, if you're using pre-built apps, a thorough background check of the vendor and security measures built into the code.

- **Secure coding practices:** Programmers should be trained in security best practices to ensure that the code they write is not only functional but secure against known vulnerabilities.
- **Regular updates:** Like devices, applications need regular updates to patch vulnerabilities and improve security features.
- **Web Application Firewalls (WAF):** WAFs can be used in conjunction with regular firewalls to inspect incoming traffic, block malicious requests, and thwart potential attacks.
- **Encryption:** As mentioned in Chapter 4, ensuring data is encrypted both at rest and in transit provides an added layer of security, making it much harder for threat actors to gain any meaningful information.

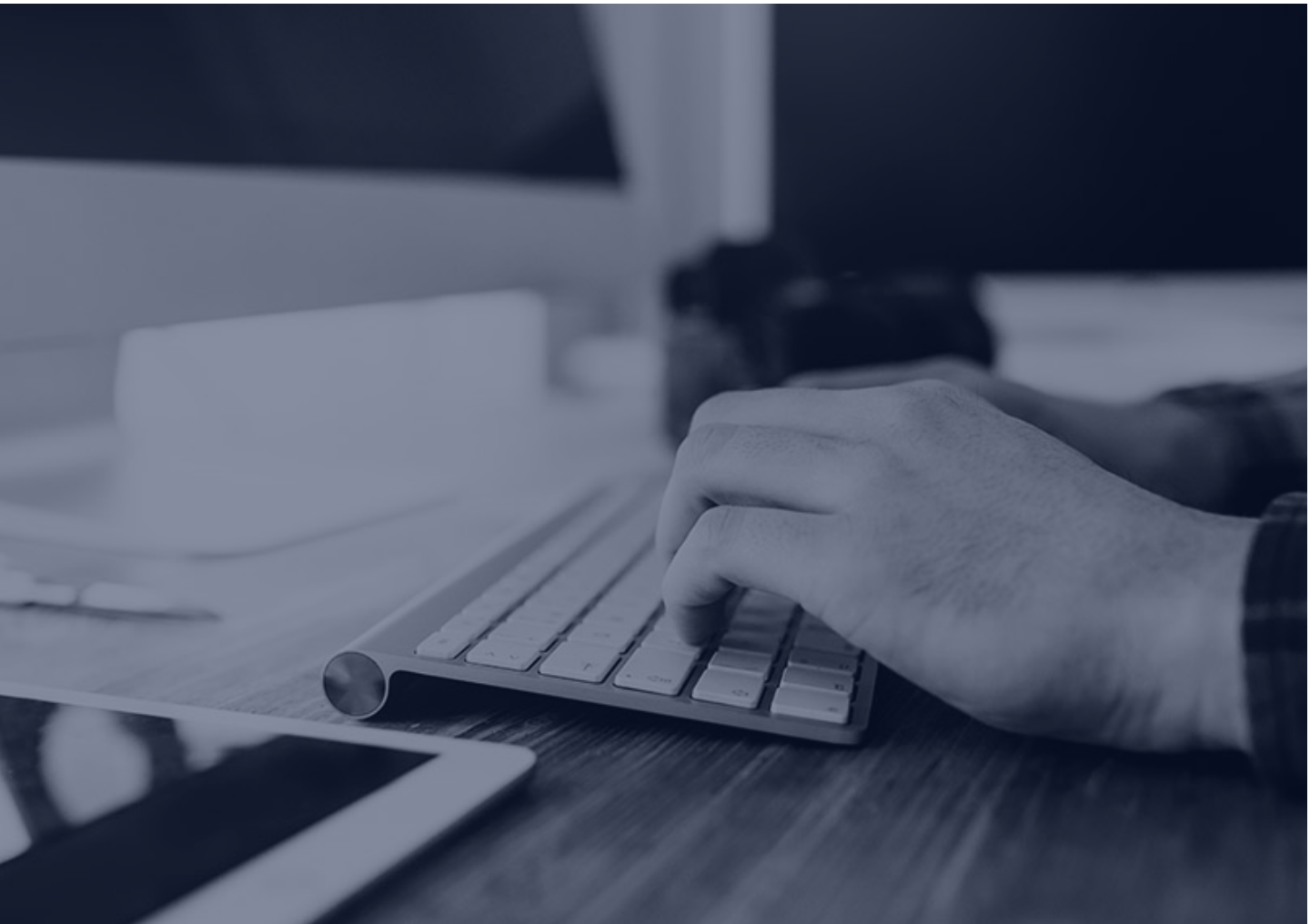
Applications are the bridges connecting users in so many different ways, and as these bridges carry precious cargo in the form of data and user trust, ensuring their sturdiness and security is vital to a strong cyber security framework.

07 CHAPTER 7: DATA SECURITY: FORTIFYING YOUR BASTIONS

From personal information and financial records, to proprietary business insights and key documents, data is at the heart of all digital operations. Its inherent value makes it a prime target for cyber adversaries. In many ways, the race to protect data and the attempts to compromise it form the core narrative of modern cyber security.

The inherent value of data naturally makes it a prime target for threat actors, and while the majority of cyber-attacks are designed around misusing data, the following are some of the most common.

- **Data breaches:** When unauthorised individuals gain access to confidential data, it leads to breaches. Whether due to malicious intent or inadvertent errors, breaches can have far-reaching consequences, from reputational damage to significant financial losses, and even legal repercussions.
- **Data theft:** Often a consequence of a breach, data theft occurs when cybercriminals exfiltrate data with the intent of selling or misusing it.
- **Insider threats:** Not all risks come from the outside. Sometimes, individuals within an organisation, driven by malice and financial incentives, or ignorance and mere oversight, can be sources of data compromise.



In many ways, the race to protect data and the attempts to compromise it form the core narrative of modern cyber security. The adage, "Don't put all your eggs in one basket," rings particularly true for data. The most effective ways to guard against data loss, theft, or compromise is to ensure you have consistent backups, and enforce policies for accessing and using data.

- **Regular backups:** Schedule frequent backups of critical data, ensuring multiple copies are stored in different locations.
- **Encryption:** As mentioned in Chapter 4, encrypting data at rest and in transit ensures that even if it's accessed by unauthorised entities, it remains unreadable.
- **Data handling protocols:** Establish clear guidelines on how data should be accessed, processed, stored, and deleted. This includes setting user permissions, determining data retention periods, and specifying data disposal methods.
- **Disaster recovery:** Beyond just backing up data, a strategy for restoring operations swiftly after a data incident is vital. This includes prioritising data restoration processes, assigning roles, and conducting regular drills to ensure efficiency.

Fortifying data bastions is a commitment to trust and privacy. Many organisations hold sensitive information regarding their clients, and if this data is leaked or stolen, the company's reputation and customer trust will take a severe hit – regardless of fault.

CHAPTER 8: MISSION CRITICAL SECURITY: SHIELDING THE LIFELINES

Every organisation has certain assets that are foundational to its operations – assets without which the organisation could grind to a halt. Identifying these mission-critical assets is the first step towards their robust protection. They could range from databases of customer information, proprietary software, patented processes, to even unique hardware components.

Recognising indispensable assets allows businesses to prioritise their security efforts, ensuring these vital assets are shielded from potential threats.

- **Intellectual Property (IP) theft:** IP can take many forms, and its theft or loss is a prime concern. Cyber adversaries often set their sights on these assets, recognising their inherent value and potential for extortion.
- **Advanced Pertistent Threats (APTs):** Prolonged and targeted attacks where an intruder gains access to a network and remains undetected for an extended period. They aim to extract information or disrupt operations over a period of time, rather than cause immediate damage.

Many of the security measures mentioned in previous chapters – encryption, backups, MFA, 24/7 monitoring, and more – are necessary to ensuring protection of mission critical assets. However, high availability takes business continuity a step further. By building redundancies into systems, organisations can ensure that if one system fails, another immediately takes its place, resulting in zero downtime.

This is often achieved through:

- **Clustering:** Grouping multiple servers so that they act as a single system. If one fails, another in the cluster can take over.
- **Load balancing:** Distributing workloads across multiple servers or systems to ensure no single system is overwhelmed.
- **Failover systems:** Automatically offloading tasks from a failed system to a backup system.

Mission critical assets are the heart of every business, underpinning innovation, functionality, continuity, and operational capabilities. Securing these assets is about resilience – the ability to bounce back rapidly in the face of an unexpected cyber incident or disaster. In essence, mission critical security is about shielding the heart and soul of your business from cyber threats.

09

CHAPTER 9: THE RECAP

Like the threads of a finely woven fabric, each security layer reinforces the other – from the human element, to mission critical assets. Recognising these intertwined relationships is pivotal, for a vulnerability in one layer can inadvertently compromise another. A holistic approach sees the layers as a cohesive whole rather than discrete entities, and is the linchpin of a strong, end-to-end cyber security framework.

The journey to strong cyber security can be complex and daunting – but you don't have to tread this path alone. Steadfast Solutions brings to the table expert knowledge, state-of-the-art tools, and a dedicated focus on ensuring your digital domains remain impregnable.

By partnering with our team of highly skilled security technicians, you're fortifying your digital defences with a comprehensive and resilient strategy that covers each layer of security with vigilance, adaptability, and continuous improvement.