J.M. ADDINGTON
TECHNOLOGY SOLUTIONS

7 ELEMENTS OF AN EFFECTIVE DEFENSE IN DEPTH STRATEGY

WHAT IS DEFENSE IN DEPTH (DiD)?

With cyberattacks growing in frequency and sophistication, businesses like yours are susceptible to data breaches now more than ever, irrespective of their size and industry. As you grow digitally and handle increasingly greater volumes of sensitive data, cybercriminals are constantly looking for ways to penetrate your defenses.

To effectively defend your business against today's sophisticated threats, amplifying your organizational security is critical. With that in mind, adopting a Defense in Depth (DiD) strategy could be exactly what you need to improve your cybersecurity posture and keep malicious cyberthreats at bay.

In simple terms, DiD is a cybersecurity approach in which multiple defensive methods are layered to protect an organization. Since no individual security measure is guaranteed to endure every attack, combining several layers of security is more effective. This layering approach was first conceived by the National Security Agency (NSA) and is inspired by a military tactic of the same name. However, in IT, the approach is intended to prevent an incident and not delay it, as in the military.

Remember not to confuse DiD with another cybersecurity concept called layered security. While layered security uses different security products to address a particular security aspect, such as email filtering, DiD is more comprehensive and includes multiple security measures to address distinct threats related to the entire IT infrastructure.

CHAPTER 1

KEEP AN EYE ON THESE THREATS

All businesses, irrespective of their size and industry, can fall prey to malicious attacks. Listed below are 23 cybersecurity threats you should be aware of:

MALWARE

Malware (abbreviated from malicious software) is a generic term for viruses, trojans and other dangerous computer programs used by cybercriminals to severely damage an IT environment or gain access to business-critical data. These programs may propagate via email attachments, website downloads or by exploiting the gaps in your operating system or other software.

RANSOMWARE

Ransomware is a type of malware that threatens to disclose sensitive data or blocks access to files/systems, most of the time by encrypting it until the victim pays a ransom amount within a stipulated deadline. Failure to pay on time can lead to data leaks or permanent data loss. Even if you pay, there's no guarantee that you will recover your lost data or won't be exploited in the future.

CREDENTIAL THEFT

Credential theft involves the unlawful acquisition of information that an individual or business uses to access websites and sensitive data. Credential theft lets hackers reset passwords, lock the victim's account, download private data, gain access to other endpoints within the network or even erase sensitive data and backups.

PHISHING/BUSINESS EMAIL COMPROMISE (BEC)

Phishing is a type of social engineering attack in which hackers appear as reliable sources to trick victims into opening phony emails or SMSs so they can penetrate those networks. Business email compromise (BEC) is a scam where cybercriminals use compromised or impersonated email accounts to manipulate victims into transferring money or sharing sensitive information.

CLOUD JACKING

Cloud jacking, or cloud hijacking, is a type of attack where cybercriminals exploit cloud vulnerabilities to steal the information of an account holder to gain server access.

INSIDER THREATS

Insider threats originate from within the targeted business. They could be past workers, suppliers or other business partners who have access to critical business data and computer systems, and they knowingly or unknowingly misuse their access. An insider threat is challenging to identify since it comes from within the organization.

DENIAL-OF-SERVICE/DISTRIBUTED DENIAL-OF-SERVICE (DoS and DDoS)

These attacks are common and easy to implement. When DoS or DDoS attacks happen, hackers flood the targeted system with a high volume of data requests, causing it to slow down, crash or shut down. An abrupt slowdown or unavailability of a website or service is the most evident sign of a DDoS assault.

MAN-IN-THE-MIDDLE (MITM) ATTACKS

A MITM attack takes place when an unauthorized entity breaks into a company's network and behaves as part of the network. It's a form of eavesdropping in which the attacker intercepts the entire conversation and controls it from the inside. Hackers do this to capture and manipulate sensitive personal information in real-time, such as personal login information, account details and credit card numbers.

DOMAIN NAME SYSTEM (DNS) ATTACKS

A DNS attack is a threat in which the hacker exploits vulnerabilities in the DNS protocol. This is a significant problem in cybersecurity because DNS is a vital component of the IT infrastructure. Hackers often target the servers that host domain names in DNS attacks. In other instances, these attackers will aim to identify flaws in the system and exploit them for their own gain.

BOTNETS

Botnets are networks of hijacked, inter-connected devices that are manipulated for scams and cyberattacks. A botnet attack is usually conducted by sending spam, stealing data, exploiting sensitive information or launching a vicious DDoS attack.

CRYPTOJACKING

Hackers use a victim's computing power to secretly and illegally mine cryptocurrency. Cryptojacking can target individual users, big enterprises and even industrial control systems (ICS). Whatever the method of transmission, cryptojacking code usually operates covertly in the background as unwitting victims use their devices as usual.

CYBERESPIONAGE

This cyberattack aims at stealing classified data from a corporate house or the government for financial, political or competitive advantages. Most cases of cyberespionage are classified as advanced persistent threats (APTs). An APT is a sophisticated cyberattack in which a hacker infiltrates a network without being discovered to acquire critical information over an extended period.

ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) HACKS

AI and ML help hackers become more efficient in developing an in-depth understanding of how businesses guard against cyberattacks. Using machine learning, hackers can tailor phishing emails to avoid bulk email lists and optimize them to encourage engagement and clicks. To give the interaction the best possible legitimacy, hackers even generate realistic images, social media personas and other content using artificial intelligence.

INTERNET OF THINGS (IoT) RISKS AND TARGETED ATTACKS

The adoption of IoT is undoubtedly on the rise. However, due to unregulated data exchange and insufficient legislation, IoT has become a favorite target for cybercriminals. Threat actors' ability to harm not only the network and software that enable IoT devices, but also the devices themselves, is a significant source of concern regarding the security of IoT devices.

WEB APPLICATION ATTACKS

Vulnerabilities within web applications allow hackers to gain direct access to databases to manipulate sensitive data. Business databases are regular targets because they contain sensitive data, including Personally Identifiable Information (PII) and banking details. Common web application attacks include DDoS, SQL injections, path traversal, cross-site scripting and local file inclusion.

ADVANCED PERSISTENT THREATS (APTS)

An APT is a sustained and sophisticated cyberattack in which a malicious actor gains access to a network and continues undetected for a prolonged duration. Most of the time, it aims at stealing data rather than damaging the IT environment. These persistent attacks are frequently orchestrated by nation-states or criminal cartels.

SQL INJECTION

SQL injection is a code injection technique in which hackers place malicious code in SQL statements. This technique can destroy a database. A successful attack might lead to the illegal access of user lists, the deletion of entire tables and, in some circumstances, the attacker obtaining administrative rights to a database.

ZERO-DAY EXPLOITS

Zero-day exploits are cyberattacks aimed at vulnerabilities that a software vendor has not yet fixed or patched. By exploiting such an unpatched vulnerability, these attacks have a significant chance of success and are tough to protect against by using outdated security tools.

SPYWARE

Spyware is software that, if installed on your computer, stealthily monitors your online behavior without consent. It can gather information about an individual or business and transfer that data to other parties. You can protect your business from spyware by using defenses like secure email and web gateways, automatic software patch management and regular employee awareness training on security.

IDENTITY THEFT AND SYNTHETIC IDENTITIES

Identity theft is a type of fraud in which a cybercriminal creates a fake account/profile like a genuine one in order to carry out scams like money laundering. Synthetic identity theft is a form of identity theft in which scammers combine real and fake information to create a new false identity. Most often, the crimes frequently go unreported or unobserved until the fraudster commits any fraud.

SOFTWARE VULNERABILITY EXPLOITS

A software vulnerability is a flaw present within software or in an operating system (OS). They can enter your network through various channels, some of which are the fault of the software vendor and others that are the fault of the user. Almost all software will have vulnerabilities in one form or another that must be fixed before cybercriminals rush to exploit them.

DEEPFAKES

A deepfake is a cyberthreat that uses artificial intelligence to manipulate or generate audio/video content that can deceive end users into believing something untrue. To make their messages seem more credible, scammers now leverage AI to create realistic- looking user profiles, photographs and phishing emails.

5G EXPLOIT

The initial overlaying of 5G technology will be over the existing 4G LTE network. Because of this, there will be vulnerabilities that the new technology will inherit from its predecessor.

CHAPTER 2

DEFEND AGAINST THREATS BY IMPLEMENTING A DiD STRATEGY

You can categorize DiD into three security control areas:

ADMINISTRATIVE CONTROLS

Your business's policies and procedures fall under administrative controls. Make sure to document your policies and procedures to ensure that the security guidelines are available and adhered to. Whether it's employee onboarding protocols, data processing and management procedures, information security policies, vendor risk management, third-party risk management frameworks or information risk management strategies, you should have clearly defined policies for all.

TECHNICAL CONTROLS

Your business's hardware or software intended to protect your systems and resources falls under technical controls. Examples of technical controls are firewalls, configuration management, disk/data encryption, identity access management (IAM), vulnerability scanners, patch management, virtual private networks (VPNs), intrusion detection systems (IDS), security awareness training and more.

PHYSICAL CONTROLS

Anything aimed at physically limiting or preventing access to your IT systems falls under physical controls. Examples are fences, keycards/ badges, CCTV systems, locker rooms, trained guard dogs and more.

CHAPTER 3

THE 7 ESSENTIAL ELEMENTS OF DiD

Here are seven key elements that must be a part of your DiD strategy:

1 INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)

A firewall is a security system comprising of hardware or software that can protect your network by filtering out unnecessary traffic and blocking unauthorized access to your data. Other than blocking unwanted traffic, firewalls can also prevent malicious software from infecting your network. Firewalls can provide various levels of protection, so you must select the level of protection your business needs.

2 INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)

IDPS monitors your network traffic, evaluates it and provides instant resolution whenever it spots any malicious behavior. Additionally, it monitors your network for any anomalies around the clock, and it notifies the stakeholders and blocks attacks if any suspicious activity is discovered.

3 ENDPOINT DETECTION AND RESPONSE (EDR)

EDR solutions operate by constantly monitoring endpoints to find suspicious or malicious behavior in real time. This is effective against internal and external attacks and is powered by innovative technologies such as machine learning.

4 NETWORK SEGMENTATION

When you divide your business's network into smaller units, you can monitor data traffic between segments and safeguard segments from one another. Additionally, by automating the process, you can restrict unauthorized entities from accessing vital information.

5 THE PRINCIPLE OF LEAST PRIVILEGE (PoLP)

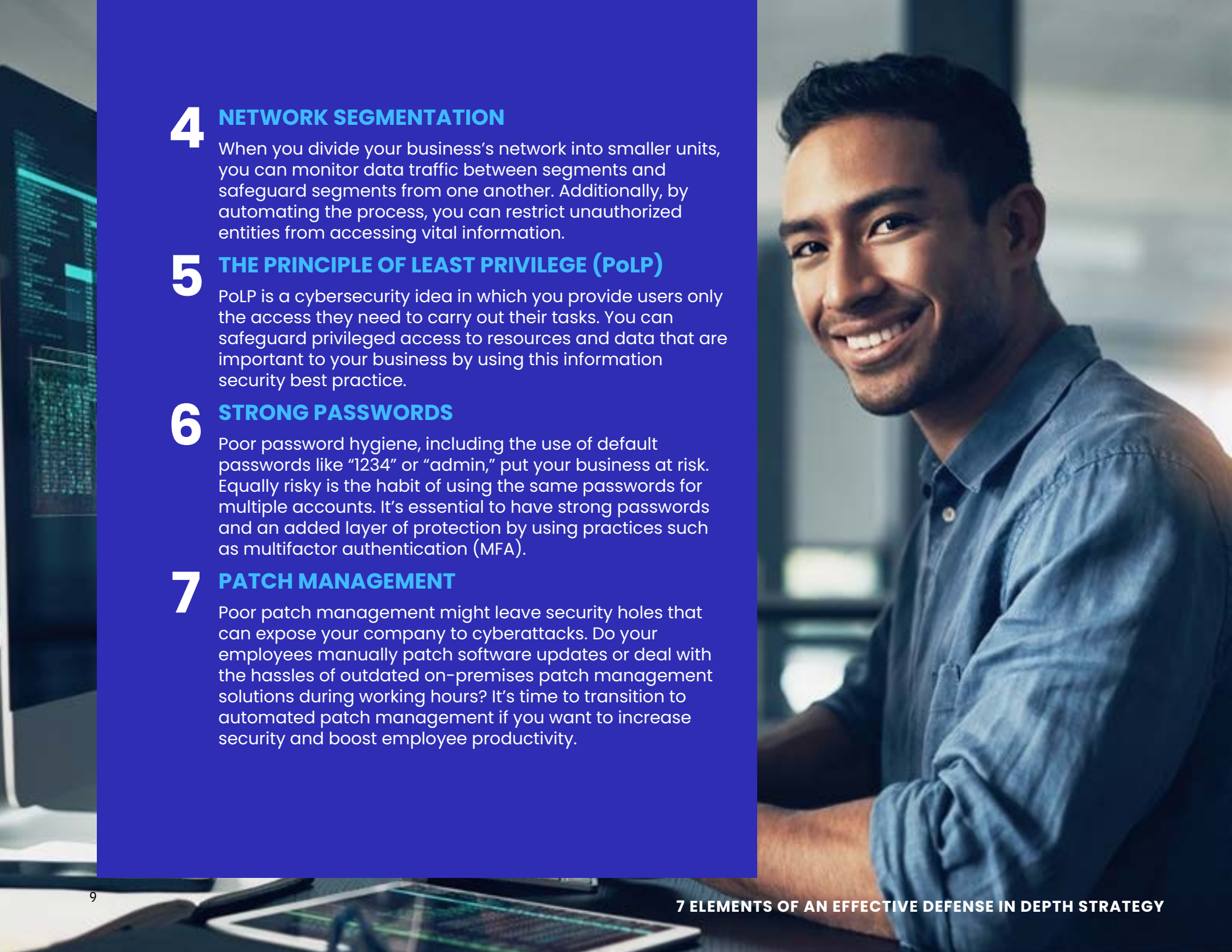
PoLP is a cybersecurity idea in which you provide users only the access they need to carry out their tasks. You can safeguard privileged access to resources and data that are important to your business by using this information security best practice.

6 STRONG PASSWORDS

Poor password hygiene, including the use of default passwords like "1234" or "admin," put your business at risk. Equally risky is the habit of using the same passwords for multiple accounts. It's essential to have strong passwords and an added layer of protection by using practices such as multifactor authentication (MFA).

7 PATCH MANAGEMENT

Poor patch management might leave security holes that can expose your company to cyberattacks. Do your employees manually patch software updates or deal with the hassles of outdated on-premises patch management solutions during working hours? It's time to transition to automated patch management if you want to increase security and boost employee productivity.



CHAPTER 4

ADDRESS VENDOR ANDCONTRACTOR RISKS

Third-party and fourth-party vendors/ contractors can put your business at risk. Since not all supply chain cases are publicized, there could be hundreds of cases that go unreported. Always remember that plugging third-party and fourth-party vendor/contractor risks is vital for the success of your DiD strategy.

It is crucial to choose vendors that are committed to delivering best-in-class security. While no system is 100% secure, some vendors demonstrate a superior commitment to excellence in security matters compared to others.

Here are some security questions you must ask a potential vendor:

- ☐ **Does the vendor have the necessary security measures in place?**

  This helps you check if the vendor can meet all your security expectations and needs. Find out if they run regular vulnerability scans, do timely system updates, etc., as per your requirement.

- ☐ **Does the vendor have all the required security certifications?**

  The vendor must provide certifications to prove compliance with the industry's security standards.

- ☐ **How and where does the vendor store your data?**

  This is a crucial question because it helps you determine whether the vendor will handle your data carefully.

- ☐ **What happens to your data once the partnership ends?**

  You must know what happens once the contract ends and you choose not to continue with the vendor.

- ☐ **Will any other parties access your data?**

  Just like you're outsourcing a few tasks to a third-party vendor, they may in turn be outsourcing some tasks to a fourth-party vendor. It's vital that you know what they share.

- ☐ **Does the vendor have a business continuity and disaster recovery (BCDR) plan?**

  You have the right to know if your vendor has a BCDR strategy in place to withstand a disaster.

- ☐ **Does the vendor have cyber liability insurance?**

  This helps you know if your vendor can pay you for damages in a worst-case scenario.

GET UP AND RUNNING WITH DiD

If you've read this far, chances are you want to ramp up your security posture in a manner that makes it especially hard for multiple threats to break through. By now, you know that a Defense in Depth (DiD) strategy is what your business needs.

If you're wondering where and how to begin, don't worry. By collaborating with a partner like us, and with our vast expertise in cybersecurity matters, you can build a secure fortress around your business's IT infrastructure.

Get started today. Contact us for a consultation to learn the next steps to implementing or updating a DiD security strategy for your business.

J.M. ADDINGTON
TECHNOLOGY SOLUTIONS