Lodestone

Lodestone Cybersecurity Primer for Small and Medium Businesses (SMBs)

Lodestone Cybersecurity Primer for Small and Medium Businesses (SMBs)

Small and medium-sized businesses have a unique challenge when it comes to cybersecurity. Unlike large corporations and government agencies that typically have formal information security teams working full time to prevent and manage cyber threats, these smaller companies rarely have the resources to systematically address their ongoing security needs.

Often, the person tasked with managing cybersecurity may not have an in-depth background in computer technology. Recognizing this, Lodestone has tailored our security consulting services specifically to the Small and Medium Business (SMB) market, bringing together our knowledge of the distinct threat landscape and an understanding of our clients' special business and regulatory needs.

Lodestone has assembled a group of security professionals who have worked in the world's top professional services firms and enterprises, allowing us to offer a high level of expertise to our clients. Our team also has industry experience from healthcare, government, military, and financial services companies. Collectively we have served companies ranging in size from 25 to 80,000 employees.

For the professional who may not have an extensive knowledge of information technology, we've put together the following guide to help provide an understanding of some of the terminology, concepts and tactics needed to successfully achieve your information security goals and objectives. We look forward to working with you to help you meet all your cybersecurity needs.

GETTING STARTED: SECURING YOUR ORGANIZATION

Securing your organization means more than turning on a firewall and paying for antivirus software. You need to focus on all aspects of the organization, considering your people and processes as well as your technology.

SECURE YOUR PEOPLE

You must first establish an effective security program that is structured around the business. You will need to prioritize your relationships with business stakeholders,

define security roles and responsibilities, and ensure that security processes are clearly communicated, tracked, and constantly improved upon.

When we think about security, we often focus on the technology involved, but that alone is not enough. It is important to keep in mind that people within an organization can present risks as well. It is much easier to exploit an individual than it is a system; all an adversary needs to do is to socially engineer someone into providing access to a system, retrieving credentials, plugging in a USB, opening an email, etc. Social engineering is the act of exploiting people by gaining their trust or by taking advantage of their ignorance to gain access to something that would be otherwise unavailable. Thus, educating the people within your organization provides an effective and additional layer of defense in a security program.

SECURE YOUR PROCESSES

You can implement several processes that will make a big impact on your organization's security. When performed properly, they can prevent the likelihood of costly mistakes. By identifying assets, controlling access to information, managing potential threats, and being prepared for the worst, you can minimize negative impacts to your business.

Identify Critical Assets

An important step to protecting the critical information and sensitive data within your organization is to first identify all of it. It is easier to secure your most critical and sensitive assets once you know what they are. These assets include any piece of information that contains names, dates of birth, Social Security numbers, medical information, proprietary information, etc. A good way to judge whether an asset is important to your organization is that if it were lost, stolen, or damaged, your organization would suffer financially or have its reputation harmed. Anything that might compromise your organization's objectives might be considered a critical and sensitive asset.

Limit Access

An organization should implement appropriate security controls based on roles and responsibilities established for individuals. This will restrict access to sensitive information to only those who need it to perform their duties. By limiting access, you can prevent unnecessary prying eyes from doing harm, whether intentional or accidental. Third-party risks make up more than 60% of breaches, so methods for

evaluating and managing vendors who may be a risk to sensitive data is essential. When evaluating and onboarding new vendors, make sure to run through a rigorous vendor approval process, reviewing their technology and business practices.

Identify and Manage Threats

By building a process to identify and manage them, you can prioritize threats or vulnerabilities based on their goals and allocate the appropriate resources to mitigate them. If resources are limited, spending too much time, manpower and money on fixing minor threats and vulnerabilities could take away from more serious ones.

Create an Incident Response Plan

Implementing incident response protocols is critical. While it would be ideal to catch and stop all threats, the fact is that there is no truly foolproof method for preventing them. If threats and vulnerabilities go unnoticed, it is important to have a method in place to investigate suspicious events related to security and privacy. Even though a problem may not seem significant, you should always treat it is as if it were. One approach would be to have forensic tools or a forensics consultant readily available. Once a breach has been identified, addressing it as quickly as possible will prevent further damage. Being prepared for the worst can save a significant amount of time and money. An incident response plan is just one part of a complete plan for business continuity and disaster recovery.

Once a breach has been identified, addressing it as quickly as possible will prevent further damage. Being prepared for the worst can save a significant amount of time and money.

Plan for Business Continuity and Disaster Recovery

If something does go wrong, having an established Business Continuity and Disaster Recovery (BCDR) plan is critical. This is much broader in scope than the incident response plan. (For more information on BCDRs, see “Plan for Business Continuity and Disaster Recovery” in the Top Security Controls section.) A recovery plan will ensure that even in the event of a disaster, your organization will continue to operate as smoothly as possible and can begin the recovery phase without delay.

Develop Secure Software

If your organization develops software, whether it is for the organization itself or to be sold as a product, it is important to implement security testing into the Software Development Life Cycle (SDLC). This allows developers to identify and repair vulnerabilities proactively, instead of having to later fix vulnerabilities from previous life cycles. This ensures that your organization is exercising due diligence in securing its product and will build your reputation for product security.

SECURE YOUR TECHNOLOGY

Protecting the technology used within your organization is just as critical as securing your processes and people. You must safeguard fundamental technology assets such as proprietary software/hardware, databases that store sensitive information, the data and information assets discussed in the previous section, and the network used to link it all together.

Network Security

The first step to securing your technology is securing the communication and availability of your network, whether it is wired, wireless or software-defined. A network is made up of desktop computers, laptops, printers, servers, and any other devices that are linked together via cables, Wi-Fi, or software in order to share resources. Anything that an organization transmits over a network needs to be secured. This could involve using any combination of the following: secure file transfer/sharing practices, encryption, network segmentation, a Virtual Private Network (VPN), Digital Rights Management (DRM), Data Loss Prevention (DLP), and protection from Distributed Denial of Service (DDoS) attacks. These are just a few of the various means available to secure a network. (For more information, please see the Glossary of Cybersecurity Terms.)

When determining how best to secure a network, many modern security strategies use data-driven security. With this approach, security teams actively collect threat intelligence and appropriately rank the risks to the organization. Resources can then be allocated most effectively, to the largest and most serious risks. This approach lowers the number of exploitations and overall security risk to your organization. (https://technet.microsoft.com/en-us/security/mt587084.aspx)

The first step to securing your technology is securing the communication and availability of your network, whether it is wired, wireless or software-defined.

Database Security

A database is essentially a collection of electronically stored data organized in a way that is easy to access and manage. Because databases hold so much data, they are attractive targets for attackers. Configuring your database properly is a very important basic step in making sure that it is secure and that unauthorized individuals cannot access it. Performing frequent vulnerability scans will show where the database is the weakest, and addressing vulnerabilities accordingly minimizes the risk of exploitation. Data should be continually monitored, tracked, and flagged for unauthorized manipulation. Encrypting your database will ensure that even if an adversary does gain access, they are unable to use it for malicious purposes.

Infrastructure Security

An organization's infrastructure consists of all its hardware, software, networks, facilities, and equipment used to manage and support its information technology services. These all must be secured as well. Storage security, hardening, configuration, and anti-malware controls all provide the foundation for security. Storage security is the group of parameters and settings that make storage resources available to authorized users and trusted networks but unavailable to other entities. Hardening refers to a process used to secure a system; among other things, this may include removing non-essential software and utilities from the computer. For example, if a system is meant only to host a website and does not collect information, then one step of hardening would be ensuring all services not specifically used to host the website are disabled on that system.

Endpoint Security

Protecting the endpoints in an organization is critical. Endpoints are devices that are connected on a network and are used physically by an end-user. Desktops, laptops, smartphones, tablets, thin clients, smartwatches, Internet of Things (IoT), printers, ATMs, smart meters, and Point-of-Sale (POS) devices are all considered endpoints. Endpoints can be protected using encryption, strong authentication, endpoint malware protection, a host-based firewall or Intrusion Protection System and device management and controls.

CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY - THE INFORMATION SECURITY CIA TRIAD

These are considered the three most important elements of security. A security policy, or control, is judged by its ability to effectively cover all three of these areas.

CONFIDENTIALITY

Information about the system or the data it is storing that is designated as secure is kept secure. This pertains to the data privacy of both systems and people as well. Anything considered confidential must be kept out of reach of the public, and those without authorization.

INTEGRITY

Information about the system, or information that it is storing, can be considered trustworthy, even in hostile situations. What percentage of absolute confidence can the system guarantee about the data it provides you?

AVAILABILITY

The resource in question will always be accessible and usable when it is intended to be so. This element is what is compromised in a denial of service attack, where a system is made inaccessible or brought offline.

TOP SECURITY CONTROLS FOR SMALL AND MEDIUM BUSINESSES

1. WHAT DO I SECURE? KNOW YOUR DATA.

Securing your data and knowing what is stored where is extremely important in your organization's overall security posture. Maintaining an inventory of assets where your data resides is critically important.

Data should also be classified and secured for proper handling. Your organization should implement ways to determine what data would be harmful if lost during a breach and maintain procedures for handling that data.

There are several types of data classifications to consider when reviewing your data and how to secure it:

- **Public** - This data may be made available to the public, or already is. This may include press releases, publicly disseminated documents and marketing materials, job postings, or anything that will not have an impact on the company if it is not secured.
- **Internal** - This information is to be protected as it includes proprietary company information, internal communications, personal employee information, or business contracts. This information is considered valuable and would be damaging to the organization or individuals within the organization if stolen.
- **Confidential** - This information is highly sensitive and must be secured with the utmost priority. This information should be considered need-to-know and can harm the organization significantly if it is breached or exposed.

Risk Assessment

A risk assessment is the process by which any threats, vulnerabilities or hazards that are present in a system are identified, analyzed and evaluated (these may include a software product, a physical workspace, etc.). Once an evaluation is complete, appropriate measures to manage or eliminate these risks are determined.

Various frameworks and standards have been developed to assist organizations in performing a risk assessment, such as SAS Nos. 104-111, NIST SP 800-30 Rev. 1, and ISO 31000:2009. These guidelines define how to determine the severity of the findings identified through a risk assessment, so that the most significant threats to the system can be prioritized. Threats are determined based on the requirements of the system.

As mentioned above, it is important to know which data/assets have the most significance to your organization. If they contain highly sensitive material, it makes sense to prioritize your security resources to those items.

2. ASSESS YOUR SECURITY POSTURE

What Is a Posture Assessment?

Posture assessments determine the overall security condition of a given system based upon methods, regulations and/or standards that the system maybe be subject to. There are several ways to carry out a posture assessment and varying degrees of technical and analytical approaches.

Penetration Test

A penetration test is performed by a highly technically skilled individual or team of individuals who identify the vulnerabilities in a system and attempt to take advantage of said issues to gain access to protected systems. The team will document the process of exploiting a vulnerability to simulate how a threat actor might try to gain unauthorized access and/or control of a system and will provide feedback on how to appropriately address the threat. There are commonly three types of penetration tests: black box, white box and gray box.

- In a **black box** penetration test, the penetration testing team knows little to nothing about the system that they are trying to exploit. This requires the penetration team to collect as much information as possible about the system without the assistance of the organization being tested. This approach most closely represents a real-world scenario, where an unknown threat actor identifies a target and attacks it.
- A **white box** penetration test is when the team is provided with all the details about the system, such as internal and external internet protocol (IP) addresses, types of hardware and software running on the system, version numbers, etc. This approach leaves the penetration testing team with less guesswork and allows them to spend more time on items known to be vulnerable based on the detailed information provided.

- A **gray box** penetration test is somewhere in between. The team is provided with some knowledge of the system that they are trying to exploit, but maybe not everything, or not all at once. This may include information like an organization's externally facing websites or employee names.

Given the rapid pace of technological change, it is important to regularly assess the security of your systems. Think of these different types of assessments as maintenance for a car or visits to a doctor. When your organization introduces a new system or process, risks and vulnerabilities may appear that would not have been reflected in a prior evaluation, so it is important to perform security assessments regularly.

3. REQUIRE STRONG PASSWORDS AND IMPLEMENT TWO-FACTOR AUTHENTICATION (2FA)

Authentication is the process of determining the identity of a user. During this process the user provides credentials which are checked against a database of authorized users. If the credentials provided match a set in the database, the user will be granted access to the system.

Making a Strong Password

The key to a strong password is length and complexity. A password should be at least 15 characters in length and contain a combination of letters, numbers, and special characters. Strong and unique passwords are paramount to achieving good security hygiene; passwords should not be reused for multiple accounts.

The problem here is that passwords often end up looking like "Sameeverytime#1", "Sameeverytime#2", "Sameeverytime#3", etc. A strong password ends up being hard to remember, and close to impossible when a different one is used for each website. This is why we advise the use of passphrases, and password managers, seen below.

Using Passphrases Correctly

A passphrase is really no different than a password, except that it is more of a sentence or phrase than a combination of random characters. The advantage of a passphrase is they're inherently long, while also being easier to remember.

Passphrases do still have their own weaknesses. When using the English alphabet, you will inherently have a high occurrence of 'a,' 'e,' 'i,' 'o,' and 'u.' Passphrases that make semantic sense "the cow jumped over the moon", also fall victim of having less entropy, or randomness. For this reason, we advise the use of phrases that don't make grammatical sense.

One example is “Red forest character triumph moon1!”, which meets most or all complexity requirements, and is much easier to remember. The association of words in a passphrase should be known only to you; the longer the phrase, the harder it is for an attacker to guess.

Storing Passwords or Passphrases

The use of a password manager is strongly recommended for storing credentials. Password managers can store all passwords, security question answers, and other personal information in one encrypted location. To access the password manager a secure password is required. These managers have online storage, browser plugins, and more, making them very accessible to even the most amateur user.

Two-Factor Authentication

Two-factor authentication is an added layer of security that requires a username and password as well as something else to verify the identity of the user. Types of authentication factors include:

- **Something you know** - a password, PIN #, or security question
- **Something you have** - a physical object that belongs to the user that can receive a token to supply the authentication process, such as a cell phone or security token
- **Something you are** - a physical characteristic of the user such as a fingerprint, retina or voice scan

The use of two-factor authentication is beneficial due to the added challenge for an attacker to bypass the multiple methods of authentication. Without the second factor the attacker would not be granted access to an account or system even if they had the correct username and password. Using two-factor authentication, a user or business can help to significantly reduce the risk for fraudulent account or system access. Keep in mind that two-factor authentication can still be subject to social engineering attacks, such as persuading someone to share an authentication factor. User training remains critical: technology alone is not enough.

4. ENCRYPT YOUR DATA

The use of encryption in any organization should be a top priority. Encryption can be implemented in emails, documents, user workstations, and servers that store company and client information. Implementing an encryption policy can be a simple task but it is first necessary to understand the different types of encryption and when to use them.

Sending an email containing confidential information internally requires one type of encryption, while protecting files on servers and workstations requires another. This is the difference between data in transit and data at rest.

- **Data in transit** – This is data that is moving between devices or across the internet. It has the potential to pass through a malicious connection or network, and so should be encrypted before being sent.
  - **Email** can be encrypted using various methods such as PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions). These confirm the validity of the data, as well as the identity of who is sending it.
  - **Instant messaging** applications use Off-The-Record (OTR) encryption to protect instant message data.
  - **Browsers and websites** use SSL/TLS (Secure Socket Layers/Transport Layer Security) to encrypt web traffic behind the scenes from the user. This is called end-to-end encryption since it is applied before sending and after receiving the data. It provides no protection against host-based threats, like a device that has been infected with malware.
- **Data at rest** – This is data that resides in the storage disks of a computer, server, or other device and is not moving between machines or networks.
  - **Computers and workstations** can be protected by full disk encryption, using tools like Filevault or Bitlocker. This can prevent an adversary from extracting data from a stolen hard drive or computer.
  - **Databases** have their own forms of encryption, usually offered by the product vendor. These treasure troves of information are common attack points for hackers.
  - **Mobile devices** can benefit from encryption as well, where applications and data related to the organization are encrypted and sectioned off from the rest of the software on the device.

5. MANAGE YOUR VENDOR RISK

Identifying the security of third-party vendors before using them is essential to your organization's security. Some questions to ask are: What types of your data do the vendors have access to? How do they store their data? What security plans do they have in place? Requirements for vendors who collect or process sensitive data such as Personally Identifiable Information (PII) or Protected Health Information (PHI) should

generally be more stringent than for those who don't, but there still may be a security risk with vendors not directly handling data (e.g., cleaning staff).

Speaking with the vendor about their security practices and sending the vendor a questionnaire to fill out are good ways for you to assess their security practices. There are many free online questionnaires that can be used to gauge a vendor's security. Google's Vendor Security Assessment Questionnaires are a good example and can be found at https://vsaq-demo.withgoogle.com/. A questionnaire provided by the Vendor Security Alliance can be found at https://www.vendorsecurityalliance.org/questionnaire2018.html.

Other companies offer vendor scorecard services and paid questionnaires, but these can be costly. Sending and reviewing the questionnaire yourself should be sufficient when assessing the vendor your organization is considering doing business with.

6. CREATE YOUR INCIDENT RESPONSE PLAN

An incident response plan is an essential part of dealing with a problem such as a data breach or other disaster. Creating an incident response plan as part of your organization's plan for business continuity and disaster recovery will help efficiently mitigate and handle issues that may arise. Beazley Breach Solutions provides a wide variety of resources to help you create and implement your incident response plan.

7. PLAN FOR BUSINESS CONTINUITY AND DISASTER RECOVERY

What is Business Continuity Planning?

Business continuity planning is the proactive, comprehensive approach to ensuring that your organization can recover from a disaster. This includes making sure that processes, procedures, services and devices critical to daily operations can still function during and after a major disaster.

A primary component of business continuity planning is implementing a data backup plan, which involves setting up a schedule to backup critical systems and data so they can be restored following a disaster. Determining how much space is needed and the length of time to store data backups depends on the volume of data being stored and the number of machines that are critical to the day-to-day functions of your organization.

What is Disaster Recovery?

Disaster Recovery is a set of specific steps an organization needs to take to resume operations after an incident. This should include guidelines for data and systems recovery, dealing with media, and steps for financial and legal action.

Why Create a BCDR Plan?

Creating a BCDR plan benefits an organization in a multitude of ways: faster recovery time following a disaster reduces loss from downtime; potential impact to the reputation of the organization is significantly lowered if it can properly and efficiently recover; and the possibility of non-compliance to contracts and regulations is avoided.

Elements of a BCDR Plan

- Business Impact Analysis and IT Risk Assessment
- Continuity and Recovery Policy and Statements
- Preventative Measures
- Business Continuity Plan
- IT Disaster Recovery Plan
- Application Recovery Procedures
- Plan Maintenance
- Plan Testing and Training Exercises

8. PATCH YOUR SYSTEMS AND SOFTWARE

Patching is the process of updating software and systems with the latest updates or fixes. If your software or computers are not patched it could leave them susceptible to malware and exploits. To ensure maximum system security, patching must be performed regularly.

As part of the patching process, a patching cycle should be enforced to ensure the latest required patches are being checked for and installed as soon as possible. A patch cycle should ensure that updates are installed every 30 days, or at maximum every 90 days. Aligning the patching cycle with your vendors' patch release cycles will ensure systems are patched as soon as possible. As an example, Microsoft and Adobe tend to release patches on the second Tuesday and sometimes fourth Tuesday of every month.

Installing patches in a test environment before installing them on all systems can provide increased stability and compatibility in the event that a patch interferes with the proper functioning of a system or service (software). To accomplish this, a test environment must be established that mimics the environment your employees and customers access. The patches are installed in this environment and then tests are performed to ensure that the systems and services are still functioning properly with the new patch installed. Once it has been verified that the new patch doesn't cause any problems, it is then installed on all systems.

9. EDUCATE YOUR EMPLOYEES

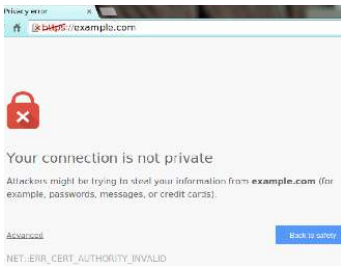
One of the most significant threats to an organization is the uninformed employee who unintentionally allows an outside attacker into your internal network. To reduce this risk, you must educate employees on cyber threats and secure-use methods for interacting with your organization's information assets.

Phishing is an important topic to cover with employees as it proves to be one of an attacker's most effective methods for retrieving sensitive information and credentials from employees. This method of attack is executed by sending emails to employees that appear to come from a legitimate source in order to lure employees into giving away their credentials or important information; the attacker can then use this information to access company data and systems. To raise awareness of phishing attacks and reinforce the importance of protecting sensitive information, you should regularly conduct educational phishing campaigns against employees and measure, track and communicate results. This way, you can reinforce good practices and eliminate those that are harmful.

Another part of security awareness training should involve the topic of rogue networks. Rogue networks are wireless access points that look like a normal wireless network. Employees should learn to never connect to public/free Wi-Fi without adequate protection, as it could potentially be a rogue network that is collecting data or downloading malicious software onto the devices connected to it. Using a virtual personal network (VPN) can help to protect against these risks, and a mobile hotspot removes the risk altogether.

Employees should also be educated about the risks of browsing unsecure websites. When users browse to unsecure websites, attackers can gain access, steal user credentials and download malware onto the employee's machine. The browser application (Chrome, Explorer, etc.) should notify users if they are trying to access an unsecure website with a message such as the one on the left.

10. MANAGE USER ACCOUNTS AND ACCESS



Managing access to systems and data can limit the possible damage done if a user decides to perform malicious actions or if their account is compromised by an attacker. A balance must be struck between giving each user the access they need to perform their duties effectively while minimizing the impact of potential malicious actions taken using the account. This is referred to as the principle of least privilege (colloquially known as "need-to-know").

Least privilege can be achieved by using well-defined user roles and recurring audits of the access each role is permitted, along with tracking which roles individual users are assigned and managing any changes to role definition and/or assignment. Each type of role (e.g. receptionist, software developer, nurse, etc.) will have a predefined set of resources which they are authorized to access based on their job duties. A software developer may not need access to patient health information, and a nurse may not need local administrative privileges on their workstation. As duties of the different roles change or new resources to which employees require access are introduced to the environment, role definitions should be updated to reflect the changes. Audits of what resources each role is allowed access to should be performed regularly to ensure least privilege is being achieved.

Once user roles are defined, each employee (or user) must be assigned to one of the roles based on their duties. A change management process should be implemented to ensure that employee onboarding, departure, or role changes within the organization are reflected in the user role the employee is assigned and therefore the access they are granted. These change requests should be verified prior to implementation to ensure they are not fraudulent.

GLOSSARY OF CYBERSECURITY TERMS

HARDWARE

Endpoint - An internet-capable computer hardware device. Examples include: Desktops, Laptops, Printers, Smartphones, Tablets, and any IoT device like a router or refrigerator.

External HDD (Hard Disk Drive) - A hard drive that is located outside a computer and is usually connected to a computer using a USB cable.

Hard Drive - A storage device used to store data on a computer.

Memory - Information or data that a computer can recall and use in short term processing. This is also referred to as RAM (Random Access Memory) in personal computers.*Portable Storage Media* - A device that can store and transport data between systems. Examples are External Hard Disk Drives and USB Drives.

Server - A computer or software that is dedicated to managing network-connected resources or services.

USB (Universal Serial Bus) - A common interface that allows communication between physically connected devices.

USB Drive (also Flash Drive, Thumb Drive) - A storage device with a USB interface.

SOFTWARE/SERVICES

Active Directory - A Microsoft Windows service that serves as a trusted source for authorization for all users, endpoints, and filesystems on the network.

Cloud - A term referencing the use of scalable, on-demand clusters of virtual machines that can share the workload of all the hosted applications. Examples include: Amazon Web Services, Google Compute, Microsoft Azure

DNS (Domain Name System) - The system that assigns human readable domain names to IP addresses.

DRM (Digital Rights Management) - A process used to protect and license digital intellectual property through the use of technological methods.

IaaS (Infrastructure as a Service) - A service model that provides hardware, storage,

servers and data center space or network components on an outsourced basis to support enterprise operations.

Linux - An open source operating system. Predominantly used in enterprise to host network server software and services.

Network File Store - A device that stores data that is accessible through a shared network.

PaaS (Platform as a Service) - A computing platform that is rented or delivered as an integrated solution or service to users over the internet.

Patch - A software update used to fix a problem in an operating system or software program.

PGP (Pretty Good Privacy) - A computer program that is used for encrypting and decrypting files and communications over the internet.

SaaS (Software as a Service) - A method to distribute software where a third party hosts an application and allows data to be accessed from any device with an Internet connection.

Shadow IT - Internet technology solutions and systems created and applied inside companies and organizations without their authorization.

VM (Virtual Machine) - Software that emulates the physical components of a computer, enabling a user to install, and run one or more sandboxed operating systems on a single device.

NETWORKING

DDoS (Distributed Denial of Service) - A type of network attack that uses multiple computer systems to overwhelm an online service causing it to crash or shut down.

Ethernet Jack/Network Drop - A networking interface that allows a computer to physically connect to a local area network.

Flat Network - A network where there is only one network segment (see Network Segmentation).

IoT (Internet of Things) - Common name for embedded devices with network connectivity. This ranges from devices like smartwatches and refrigerators to more common equipment like routers and printers.

IP (Internet Protocol) Address - A logical numeric address that is assigned to every computer or device connected to an IP based network.

LAN (Local Area Network) - A network, or series of networks, all connected to a parent hub or switch. This can be as small as a Wi-Fi hotspot or as large as a university network.

NIC (Network Interface Card) - A computer hardware component that allows a computer to connect to a network either through a wired or wireless connection (Wireless NIC).

Network Segmentation - Splitting a computer network into subnetworks, where each subnetwork is a network segment. A flat network is a network where there is only one network segment.

Packet - A unit of data that travels over a network.

Router - A device that analyzes data packets and determines whether data must be transferred from one network to another.

S/MIME (Secure/Multipurpose Internet Mail Extensions) - A technology that allows emails to be encrypted.

Switch - A device that receives incoming data packets and redirects them to their destination on a local area network.

TLS (Transport Layer Security) - A protocol that provides privacy and security between communicating applications.

VPN (Virtual Private Network) - An encrypted tunnel that connects a user to a remote "local" network. This allows access to internal network resources like file servers, email, and printers.

WAN (Wide Area Network) - A connection of one or more switches or hubs, connecting their respective local networks. The "Internet" is a WAN.

Wireless Access Point - A device on a Local Area Network (LAN) that allows wireless-capable devices to connect to a network.

Wireless NIC - A computer hardware component that allows a computer to connect to a wireless network.

Wireless Repeater - A device used to extend wireless network signals.

INTERNAL SECURITY

DLP (Data Loss Prevention) - A strategy for making sure that end users do not send sensitive information outside the organization's network.

EHR (Electronic Health Record) - An electronic record of a patient's medical history that is maintained by a medical provider.

Encryption - The process of using an algorithm to transform information to make it unreadable for unauthorized users. The following terms are used when talking about encryption:

Data at Rest - Data that is stored in stable destination systems.

Data in Transit - Data that is being used in an IT infrastructure.

Network Encryption- The process encrypting data transmitted over a computer network.

Host-Based Encryption - The process of encrypting data using software on a computer.

Asymmetric Encryption - An encryption scheme which uses two different keys, public and private. The public key is for encrypting, and intended to be widely distributed, and the private for decrypting, known only by the owner.

Example: Alice wants to send Bob a private message. Alice protects her message with Bob's public key, and posts in on a public website for everyone to see. But, only Bob can decrypt the message with his private key, so only Bob knows what the message means.

Symmetric Encryption - An encryption scheme with one key, used for both encryption, and decryption. Just like a chest with a lock and key.

Public Key, Private Key Encryption - Another name for asymmetric encryption

Endpoint Anti-Virus - Software that detects, prevents and removes viruses and other malware from a computer.

Firewall - A piece of hardware or software that unauthorized access to or from private networks.

IPS/IDS (Intrusion Prevention System/Intrusion Detection System) - A system that monitors a network for malicious activities such as security threats or policy violations.

PHI (Protected Health Information) - Individually identifiable health information that is found in electronic media, electronic media transmissions and any other electronic medical record.

SIEM (Security Incident and Event Management) - The process of identifying, monitoring, recording and analyzing security events or incidents in an IT environment.

SSL (Secure Sockets Layer) - A protocol used for secure transmission of documents over a network. An SSL Certificate is a form of authentication used to validate the security of a website and provide protection for the identity of website users.

WAF (Web Application Firewall) – This protects web application infrastructure from attacks coming from the internet and external networks.

Web Proxy - A process to filter requests from the web to make sure no dangerous internet traffic gets through to a system browsing the internet.

SECURITY SERVICES

Managed Security Services - A provider that deploys and manages a security infrastructure. Their services tend to include: SIEM Monitoring, Patch Management, Endpoint Monitoring, Firewall Administration.

Mobile Application Assessment - An assessment of the risks to the security of a mobile application.

Network Penetration Test - The method of testing by simulating malicious attacks from an organization's internal and external users to check for vulnerabilities in an organization's systems.

Reverse Engineering Assessment - Analyzing software to identify and understand what it is composed of and whether it has any vulnerabilities.

Risk Assessment - An assessment that evaluates the potential risks that may affect an organization from a security perspective and provides recommendations to mitigate those risks.

Security Implementation - A cybersecurity methodology for standardizing security

protocols and implementing secure processes and equipment.

Security Maturity Assessment - An assessment of an organization's security processes, implementation, and policies to determine how well it can defend itself from threats.

Vulnerability Assessment - An assessment that identifies, quantifies and ranks possible threats to an organization.

Web Application Assessment - An assessment that tests and analyzes a web application for vulnerabilities.

RESOURCES

Secure Your Technology—Information on Implementing a Data-Driven Computer Security Defense:
https://technet.microsoft.com/en-us/security/mt587084.aspx

Vendor Security—Sample Questionnaires

https://vsaq-demo.withgoogle.com/

https://www.vendorsecurityalliance.org/questionnaire2018.html

www.lodestone.com
263 Tresser Boulevard
9th floor, Suite 959
Stamford, CT 06901