CyberLeet Technologies

Company Training Manual

CyberLeet Technologies

Company Training Manual

Prepared by:

Lorenzo Mateo

MANUAL OVERVIEW

You are the training manager at CyberLeet Technologies, a midsized firm that provides cybersecurity services to other businesses. CyberLeet's core customer base is sole proprietorships and other mom-and-pop shops that are too small to have their own IT departments and budgets. Generally speaking, your clients have a reasonably high risk tolerance, and put a premium on the functionality of their IT systems over stringent security measures. However, you also have clients that must protect highly sensitive information in order to continue operating successfully. For example, CyberLeet supports a few small public-accounting firms that need to maintain important tax-related information, as well as several day-care businesses that must keep children's health records private while allowing necessary access for certain caregivers. In the past year, CyberLeet has experienced rapid growth, which means you can no longer personally provide one-on-one training to every new information security analyst as they are hired. Therefore, you have decided to create a training manual that will explain to the current and future cohorts of new hires the essential principles and practices that they must understand in order to be successful in their role as information security analysts at CyberLeet.

Manual Layout

There are four sections in the manual, which cover all the components of a new employee training manual. As the training manager, you must complete each section using information you learned in this course. Refer to the background information on CyberLeet and apply the appropriate information that best matches based on the size of the company, the value of cybersecurity, and its core tenets. Apply best practices of cybersecurity principles for addressing the common threat scenarios of a sole proprietary business. The main sections of the manual you are responsible for completing are the following:

- Introduction
- Core tenets of cybersecurity
- Developing cybersecurity policies
- Threat mitigation scenarios

SECTION 1: Introduction: Welcome to CyberLeet

1.1 Introduction

We specialize in helping organizations meet their security needs. Our knowledgeable security experts provide technical assistance and training on proactive security solutions, preventing data breaches, cyber-attacks, and any other cyber-security topics. Other services we provide are monitoring networks and applications for malicious activity, managing security devices (routers, switches), responding to potential attacks in a timely manner. Maintain compliance with Federal and/or State laws. Without these services in place our client's data would be vulnerable to potential attacks. We are here to mitigate and respond to any cyber security mishap.

The reason there is demand for information security in business environments is some businesses receive and store sensitive information such as healthcare records, transactional records, and identifiable information (ex. Social Security number). This information must be protected.

The impact of cybersecurity issues can be catastrophic. Depending on the attack customers personal information or patient's medical records can be exposed. Leaving them vulnerable to possible identity theft. Network attacks can cause system downtime and data loss. Companies may go into financial hardship with revenue losses and the possibility of arbitration due to data breaches.

1.2 Your Role at CyberLeet

Information security analysts will plan and carry out security measures to protect client's computer networks and systems. Responsibilities are continually expanding as the number of cyberattacks increase.

Duties Include:

- Monitor the network for security breaches and investigate a violation when one occurs.
- Install and use software, such as firewalls and data encryption programs, to protect sensitive information.
- Prepare reports that document security breaches and the extent of the damage caused by the breaches.
- Conduct penetration testing, to look for vulnerabilities in the system.
- Research the latest information technology (IT) security trends.
- Plan and carry out ways of handling security.
- Develop security standards and best practices.
- Recommend security enhancements to management or senior IT staff
- Help computer users when they need to install or learn about new security products and procedures.
- Conduct Training on preventative methods in cybersecurity.

Once assigned to a client the Information Security Analyst will conduct himself or herself in a professional manner working diligently with the client to ensure data is safe and secure. Securing the client's data is high priority.

1.3 Purpose of This Manual

Information Security Analyst should not deviate from the guidelines covered in this manual. Principles and practices outlined reflect best practices and standard implementation of cybersecurity in a business environment. The manual illustrates clear and concise content on methods, principles, and practices for current and new Information Security Analyst to follow.

If the guidelines and principles are not implemented appropriately it could lead to a potential breach of CyberLeet data or the business client data. Breaches or cyber-attacks cost a company or its clientele, legal fees, system downtime, lost productivity, or reputation damage which could cost the company loss of business in the future.

SECTION 2: Core Tenets of Cybersecurity

2.1 Confidentiality

Confidentiality is defined as actions that are intended to protect against unauthorized discovery of secure information. As used in a business context people with specified rights within a system can only view certain aspects of data or application of information. This ensures confidentiality as data can only be viewed by authorized users. For example, a person with **administrative privileges** logs into an online healthcare systems database. This privilege level gives the person access to all healthcare records in the database. As opposed to a person who logs into the same system with **patient privileges** could only view their record in the system. (Techopedia Inc, 2019)

2.2 Integrity

Integrity involves protection from unauthorized modifications (e.g., add, delete, or change) of data. Data systems in most companies must maintain accuracy, consistency, and trustworthiness. A specific implementation to secure data integrity would consist of hashing. Comparing received hash data with a hash version of the original data. If both hashes produce different results within the received transmission data was altered in some fashion, requiring specific actions to be taken. (Techopedia Inc, 2019)

2.3 Availability

Availability is protecting the functionality of support systems and ensuring data is fully available at the point in time or period requirements by its users. In a business environment this would equate to on-site or off-site servers performing regularly scheduled backups. The preference is to have mission critical data using off-site backups. As to lessen downtime if a natural disaster, massive data attack to the network, or any other unforeseen incidents. Companies can restore any type of data from these regular backups. (Techopedia Inc, 2019)

SECTION 3: Cybersecurity Policies

3.1 Password Policies

Confidentiality password protections safety measures ensures privacy is enforced at each connection of data processing stopping unauthorized discovery of secure information. Password Integrity protections make sure the data is secure and kept intact given authorized personnel access only. Availability guarantees access to the data when needed providing password combination can be verified.

Account access on various client's system such as networks or internal applications will need to have control access management. The client should specify the level of access the user will need to complete specific task. Users should have enough access to perform job duties. For example, a user performing data entry in an internal application should not have database administrator rights.

Password Policy Guidelines:

- Password complexity - passwords should be at least 8 characters long, must contain both upper and lower-case letters, a number and symbols.
- Password System Reset - systems should force passwords reset every 20 days
- Account lockout threshold - systems will lockout users accounts after several password attempts. Access to the user account will be restored after several minutes is passed. For users accounts to be restored in a timely manner and authorize request support ticket must be submitted.
- Password management - security analysts and the companies network administrators are the only people with the authority to restore and delete a user's password.

3.2 Acceptable Use Policies

Confidentiality through Acceptable Use Policies will make sure authorized personnel are using computing equipment and network services in a secure manner to protect internal data system.

Acceptable use policies will ensure authorized users are familiar with and implementing the password policies of the company. The company will keep track allowing only a certain number of off-site computing and mobile equipment to access network services. This will ensure only authorized employees are using computing and mobile devices as intended protecting network services preserving data integrity.

Availability authorize personnel adhering to the Accessible Use Policy will have access to the company’s internal data system.

Acceptable Use Policy Guidelines:

- Company prohibits use of public Wi-Fi on company devices
- Employee should never share passwords or use someone else’s username and password combination to sign into a computing device that was not assigned to them. This refers to on-site and off-site computing equipment.
- Employees will not use their personal computing or mobile devices to access the company network resources.
- Employees will not access these restricted sites on the company Internet (Facebook, Twitter, Pinterest, Instagram, Tumblr, Reddit, Flickr, All porn, gambling, and illegal activity websites) on any internal or external computing or mobile devices.
- Employee should never open any attachments or links they were not expecting. If a suspicious email is received, alert your immediate supervisor.

3.3 User Training Policies

The User Training Policies will help users on becoming more cognizant of companywide security policies and procedures to maintain the confidentiality, integrity, and availability of the company's information systems. These policies will train employees on techniques used to identify potential cyber-attacks, phishing schemes, and physical security threats such as piggybacking, and tailgating. These policies will also train employees on security procedures to follow if a data breach were to happen.

User Training Policy Guidelines:

- Employees will have mandatory training on how to recognize phishing schemes from emails and possible data breach through unauthorized account use
- Employees will have mandatory training on all companywide security policies, password policies, acceptable use policies, federal and state laws, regulations, and guidelines deemed necessary.
- Managers and supervisors will have high-level advanced training on prevention of cyber-attacks, security policies, password policies, acceptable use policies regulations, and guidelines.
- All employees will have a mandatory training on the importance of recognizing unauthorized personnel.
- Depending on the client's needs the security analysts will customize training as deemed necessary for the company.

3.4 Basic User Policies

Basic User Policies encompasses the physical security CyberLeet maintains. These policies ensure only authorized personnel are allowed in CyberLeet facility. Having employees confirm their identity lessens the chance the various characters infiltrating the facility potentially gaining access to sensitive information. The confidentiality, integrity, and availability of information systems with these policies will be protected from unauthorized personnel.

Basic Policy Guidelines:

- Employees will be required to check in at the security gate before entering the facility.
- Employees must present their Identification (ID) badge.
- Employees are required to have a company parking sticker.
- If an employee forgets or loses their ID badge they must check in at the front desk. There a temporary badge will be issued.
- All visitors to the facility will check in at the front desk and be issued a temporary badge.
- Visitors are not allowed in secured areas and must be escorted around the facility by authorized personnel.
- Employees will not take-home equipment (computing or mobile devices etc..) unless authorized by an administrator. If authorized equipment must be signed out before leaving the property.

SECTION 4: Threat Mitigation Scenarios

4.1 Theft

Scenario: *One of your client's office has experienced two break-ins, which resulted in the theft of employee laptops. In the first incident thieves were able to break in through a ground-level window around evening time. The second incident happened during the day where thieves walked into the business area and removed two laptops.*

In dealing with physical security threats CyberLeet Information Security Analysts must implore three major factors to address the above scenario. Three factors are prevention, detection, and recovery.

- **Prevention** (Controlling) - securing and controlling the access point to the business environment, internal computer system, and network. These areas should be extremely difficult for physical and non-physical attacks.

  Perimeter barriers such as fencing, barricades, and secure area signs should be considered for building points of entry such as parking lot and ground-floor windows.

  Internal Access Control - includes door security technology such as mantraps, turnstiles, and double door entry. Door locking technology should also be considered, locking technology such as pick resistant locks, keypads, electronic system use with key cards or ID badges, and biometric locks used in conjunction with fingerprints or iris scans. Physical access log should be implemented for visitors and employees who have forgotten their ID badge.

  Employee awareness - employees should be trained on the dangers on letting unauthorized persons access the building without proper credentials.

- **Detecting** - if thieves have bypassed all prevention systems. As an Information Security Analyst, you must determine how and when the security was breach or broken into.

  To detect recent breaches video cameras should be installed at all designated secured locations. The cameras should maintain live and recorded video streams which can only be accessed by security personnel. A daily security systems backup should be implemented with backup storage housed at an off-site facility or cloud service. In playing back the recorded video stream a suspect may be identified.

  Reviewing all physical access logs. Access log should be dated and written clearly for comprehension. Visitors or employee should sign in with their printed first and last name, the department they will visit, floor destination, date, time in, and time out.

- **Recovery** (mitigating threats) - having analyse all security systems for evidence of break in or breach, a plan of action must be put in place on how the incident or multiple incidences happened in the first place. The plan should outline the potential flaws in the current system. For instance, the two incidents of theft that targeted the client’s employee laptops was perpetrated as a physical breach therefore perimeter barriers, internal access control, and employee awareness should be reviewed and constructive recommendations or solutions to the gaps or lapse in physical security should be re worked and implemented.

4.2 Malware

Scenario: *One of your client's staff has been flooded with phishing emails targeted at individuals and related to current business opportunities for the company. These messages are linked to malware and sent by known threat actors.*

In dealing with Malware security threats CyberLeet Information Security Analysts must implore three major factors to address the above scenario. Three factors are prevention, detection, and recovery.

Malware (most time malicious code) is a type of software or injected code designed to take over or damage a computer without the user's knowledge or approval. A common attack to infect systems, cybersecurity attackers embedded a type of malware in the email format sending it to unsuspecting users. (TestOut, 2019)

- **Prevention** *(Controlling) - to prevent malware infection install antivirus, anti-spyware, anti-root kit, anti-malware, and personal firewall software. Perform regular scheduled scans to look for malware. Install the latest patches for operating system. Use the latest version in patch level for web browsers. Train users not to download files or click attachments from unknown suspicious sources.*
- **Detection** - most antivirus, anti-spyware, anti-root kit, and anti-malware software come equipped with scanning tools which will detect and isolate any malware issues found on the system.
- **Recovery** (*Mitigating threats*) - in the above scenario the user should be trained not to open any attachment or files associated with suspicious emails. If malware has occurred in the client system, applications may need to be reinstalled, or even the entire operating system from scratch. The organization should be equipped with an imaging solution with the network administrator can quickly re-image one or multiple machines.

  Most antivirus software has remedy functions. Antivirus third-party software will automatically or semi-automatically resolve issues. Prompting the user of what actions to take either quarantine the file or delete the file if a virus or malware is detected.

4.3 Your Choice

Scenario: *One of your client's employee received a call from someone identifying themselves as a high-level manager. The person is requesting the employee give them their username and password and their security badge number as they are locked out of the building and the network.*

To start addressing this issue the CyberLeet Information Security Analysts must adhere three major factors to address the above scenario. The three major factors are prevention, detection, and recovery.

- Prevention (Controlling) - employee should have extensive cybersecurity awareness training on how to deal with solicited requests of this type. All employees should be held accountability for their role in the organization's cybersecurity efforts.

  According to the User Training Policy: Employees will have mandatory training on all companywide security policies, password policies, acceptable use policies, federal and state laws, regulations, and guidelines deemed necessary.

  After training and testing Users should be proficient in addressing a supposed high-level manager asking for network system credentials and ID badge information by referring them to the IT help desk or their immediate supervisor.

  When an employee voluntary or involuntary leaves the organization. All access to the network, applications, and physical security should be disabled or terminated.

- Detection - if security credentials were inadvertently given to an unknown source. Network monitoring of users logging into the system should be reviewed for any anomalies such as irregular login in and out times. A correlation between when the user logged in and an intrusion was detected by the system. Trace incoming requesters call to a valid company phone number.

- Recovery (Mitigating threats) - if an employee username and email password is compromised delete user account from the system. Disable all privileges to internal and external security areas. Report username and password exposure to the appropriate organizational authority.

If necessary, conduct an exit interview for termination of an employee who violated the organization's security policy. The employee should recognize the violation and recognize that it was the grounds for termination. The employee should provide a signature agreeing to the reason for termination.

SECTION 5: References

Techopedia Inc. (2019). CIA Triad of Information Security. Retrieve from:

https://www.techopedia.com/definition/25830/cia-triad-of information-security

Test Out Corporation (2019). Malware Protection Facts. Retrieved from: http://testout.com