CyberLeet Technologies

Company Training Manual

CyberLeet Technologies

Company Training Manual

Prepared by:

Scott Allison

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

In Section One, describe the organization. Provide a short history of the company, define the way it operates, and describe its place within the industry and the community it serves. Follow the prompts to complete each section. All prompts should be deleted prior to submitting this section.

SECTION 1: Introduction: Welcome to CyberLeet

1.1 Introduction

Welcome to Cyberleet. We are a cybersecurity firm that provides service to other businesses. As you may know our clientel are primarily small businesses such as restaraunts, small clinics, accounting firms, and other local small business practices. As the technology evolves so do threats at an incredible rate. It's unreasonable to assume that those who's profession is not within the technology field can be expected to keep up. That is where we come in. Offering expertise and security to those who need it and protecting their information. What we offer is peace of mind from threats people may not even know exists, but will suffer the repercussions of regardless of that should the worst come to pass.

Should their information be compromised medical records could be stolen, personal information be manipulated, bank accounts be tampered with or even erased! This is without mentioning the time lost trying to fix this damage, or business lost as a result of destroyed trust from such an intrusive issue.

1.2 Your Role at CyberLeet

Your role here at Cyberleet is to aid these people in keep themselves, their livelihood, their peace of mind and potentially even your own information secure and safe. As a security analyst you will be responsible for maintaining the clients hardware both on company grounds and potentially at their place of business. Whether through remote access or, hopefully not, physically going there. Additionally it's your responsibility to keep all softwares up to date. As well as perform routine checks and ensure the there is no active sniffing being done to the connection, no loggers or other malicious material is present. The client may have questions. Answer them to the best of your ability.

1.3 Purpose of This Manual

While you perform your duties remember that the tenets, guidelines, and suggestions outlined in this manual are here to make the job easier, safer, and uphold Cyberleet and cybersecurity in general's principles. By applying the tenets outlined in the following sections the rest of your responsibilities become that much easier. A job done right is a job that doesn't need to be done twice. Disregarding them has historically lead to breaches in data where very secure information(like that mentioned in the previous section) was stolen. There is a lot at stake so it's important that everyone in the company and industry follow the same protocols.

Beyond the terrible repercussions of lost data, the client will lose faith in our business and we as people. Given we are centered on small businesses and ergo small communities. That's not good.

A widely applicable security model is the CIA triad, standing for confidentiality, integrity, and availability. There are three key principles that should be guaranteed in any kind of secure system. In Section Two, describe the significance of each area as directed in each designated area. Follow the prompts to complete each section. All prompts should be deleted prior to submitting this section.

SECTION 2: Core Tenets of Cybersecurity

2.1 Confidentiality

This tenet is to protect against unauthorized access of information. This is significant because that is largely the whole point of cyber security. To protect information. Unauthorized access to personal or confidential comes in many forms such as an attacker obtaining login information from a user, and gaining access to data such as medical records or sales data.

Imagine that you ignored confidentiality protocols and gave access to your businesses sales data to a stranger. That person could then take that data and rob you blind.

2.2 Integrity

This is centered on protecting assets from tampering. Such as the adding, removal, or deletion of data. This is critically important to anyone and any business. Without following this tenet properly and obeying the protocols set for it the client is open to potentially disastrous consequences. Deleting doctors appointments, pill reminders, flight details, band bank accounts are the most damaging but not at all the only risks. Following this pillar involves proper routine maintenance or system firewalls and securities, as well as permissions for files from user profiles or groups.

2.3 Availability

This tenet is based on the principles of protecting systems and keeping data available at all times for users. As we are simply meant to secure data, not decide when its up, down, or otherwise accessible, it's up to us to ensure said data is never obstructed by our services. Following this tent ensures smooth, always usable data. Ignoring its practices could result in unavailable data and some businesses grinding to a halt as a result, or worse. Imagine a scenario where in a small clinic has an emergency operation to perform and needs the profile of a patient in order to decide what medications said patient is current prescribed. If that data is unavailable that patient could die.

Creating effective cybersecurity policies will make visible changes to how the organization operates. Rely on the information presented in this course to develop the necessary standards and frameworks of effective cybersecurity policies. Follow the prompts to complete each section. All prompts should be deleted prior to submitting this section.

SECTION 3: Cybersecurity Policies

3.1 Password Policies

One of the most important aspects of our business is ensuring the security for our clients. In order to do this effectively they, and we, must have proper password protection. As their adviser you must ensure that all passwords on both their security applications and users follow good protocols such as upper and lower case letters, numbers, and special characters. Remind them that these passwords will cycle every few months and that too many incorrect attempts will result in a lockout. Ensure that users o varying levels of authority have proper privileges but only whats necessary. Creeping privileges are a big risk.

Do not let them keep their passwords somewhere unsecure. Such as on paper in the office, on their phone, or any other unsecure device. While we will do everything we can to protect the sanctity of our clients no amount of defense will matter if an attacker has the keys. Remind them of social engineering practices such as friends or colleagues watching over their shoulder during their sign in.

Additionally if the business you are advising highly protective of their data consider Intune, or other policy enforcing software. More is discussed later but one of the features of this type of enforcer is that it allows a secondary password to gain access to a device or system.

3.2 Acceptable Use Policies

Another issue with many businesses is what constitutes useful company time. While it's reasonable to allow an employee to bring their personal devices to work. Allowing them access to the wireless network comes with a huge security risk. Creating a guest network is recommended. This will allow them free reign over an unsecured network but not grant access to other, work related computers on the private business networks. If the user desires to work ON their personal devices they will need to secure their device properly with features like Intune. Their devices should possess a lockout timer for idleness, disable functions unrelated to work such as the mic, camera, and the ability to copy data. These are all potential security risks. Additionally an MDM structure for their business may aid them as well.

Additionally web addresses and content should be barred and limited through control modules like Cisco in order to regular what content on the web is viewable during business or leisure hours. Restricting access to what the business deems inappropriate.

3.3 User Training Policies

If the business prefers to include personal devices in their workforce it is highly suggested to implement an NAP to prevent their devices from being too great of a risk. An NAP will ensure each device that connects is up to par, and prevents those that aren't from doing so. It is crucial that each employee of that business understand this process to limit the number of phone calls we get.

As a security specialist you are in charge of not just their securities but their training with these services as well. Ensure that each employee, management included, are up to date on at least the purpose and basic understanding of what services like Intune and Cisco are, along with why there is a guest network.

Trainings would occur every time a new major update was pushed out and additional training for employees who prove unable to understand it, or continuously run into problems. The employees will also need to know where they can use their company devices, should they be given out and geofencing be used.

3.4 Basic User Policies

ID at work is as important as any other means of security. By requiring it and other forms of ID the business is that much more secure from potential risks. Some businesses may consider allowing guests into the premises. If so, ensure that the employees understand that the guest is to use the guest network only, be given a guest account for networking usage. As their device unsecure and a risk for them and their business. Ensure that each employee also understands that access to restricted areas like where the servers are located is prohibited.

While it's also fun to explore a business the management must understand that access to servers and sensitive equipment is prohibited entirely. It's a massive security risk to allow just anyone access to this hardware as regardless of how secure our company is in blocking usb ports of setting up protections. There is little to be done about literally stolen hardware.

A threat-intelligence service provides analyzed, actionable threat information to help organizations defend against known or emerging threats before systems may be compromised. In this section, you will create three mitigation scenarios. The first two mitigation topics have been chosen; however, the third one is your choice. Follow the prompts to complete each section. All prompts should be deleted prior to submitting this section.

SECTION 4: Threat Mitigation Scenarios

4.1 Theft

With regard to the case of the missing laptops where in a thief simply walked in and took what they desired. A keycard security feature would need to be implemented in order to prevent entry to the building altogether. In addition a sign in book at the lobby for guests entering with a camera aimed at it ensures that should anyone make it into the building, their face is recorded. A system in place such as Microsoft Intune on company hardware would allow for stolen goods to be require additional login for access, or even wiping should it be necessary.

With regard to the thief who entered through the first floor window it much more difficult to prevent. However, by having laptops returned to one room that requires a keycard to even open. Such as a storage closet, it would prevent a thief from having access without furthering damaging the property. Locking the windows, or lacing them with window laminate would deter most thiefs entirely.

For both cases, Microsoft intune and geofencing would be ideal security measures to ensure that unwanteds do not gain access to company data.

4.2 Malware

To handle phishing and common malware practices the first step is limiting exposure to risky material. A DMZ and a false area such as a honeypot are invaluable assets to both screen users and collect information on attempting attackers. Additionally, restricting access from the primary network from guests and employees on their personal devices dramatically reduces the risk for a company's infrastructure.

4.3 Your Choice

A common thread one may face while under employment is that of an inside operative, or a spy. One who seeks to get into the company legitimately and then leak out information. Protecting your business from this threat is rather difficult, as they are legitimate employee legally. However there is a way to protect the business. By restricting the ports on physical devices for servers and others one limits the potential risk having physical access has. Additionally by configuring switches properly one can restrict access to certain IP's except from certain IP's. For example,only allowing access from the IT Admin's terminal, but blocking all others from the business. A keycard system with varying degrees of authority access could prevent a would be spy from having physical access to the servers as well. So long as those with access are careful! Of course, cameras are helpful to should the potential spy be venturing into areas they shouldn't. Finally, keep careful monitoring of the permissions for privilege creep to prevent accidental access to vital documents.

SECTION 5: References

Prompt: If applicable, list all references used in the creation of this document here. References must be in APA format.