Cyber Security Analysis of the “Green Box” Company

Author: Yasmin Morshed

October 2021

Contents

Executive Summary

This report analyses the cyber security situation of the “Green Box” company. Cyber security's core function is to protect the devices we use and the services we access-both online and at work-from theft or damage. According to the latest Cyber Security Breaches Survey 2021, “four in ten businesses (39%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months.”[1] Therefore, it is essential that vulnerabilities, especially critical ones, are managed as soon as possible. Three different kinds of controls have been suggested: physical, procedural and technical. By implementing the changes suggested below, the company will be significantly more cyber secure.

Physical Controls

The suggestions here will prevent an attack through the use of something tangible.

1. Identification

✗ Anyone could easily enter the company, posing as an employee or picking up the printed documents, gaining access to information. Authentication is essential.

✓ Employees should always wear lanyards with an ID card. This card can be used at the entrance of the building to grant access and log their entry/exit. It can also be used for picking up printing jobs.

2. Data Centre Security

✗ Server and router are on side table, easily accessible and not protected from damage. Server damage means whole business goes down.

✓ The server must be in a designated area. There must be additional controls utilised to ensure it is working and safe. Smoke and water detectors must be installed in the area. There should be a way of monitoring any power failure or overheating.

3. Reception Area

✗ After entering the building, I could easily go straight to the MD’s office to introduce myself.

✓ Control visitors to the facility, validate authorized access to the company.

4. Fires and Flooding

✗ The servers and data are at risk if there is a fire at the company. Risk from flooding due to problems in plumbing can cause damage to equipment.

✓ Appropriate fire safety in place such as fire-proof cabinets. Regularly check plumbing.

5. Security Camera

✗ Vandalism or theft going unnoticed, entry of unauthorised people

✓ CCTV cameras should be installed inside and outside the premises.

6. Security Guard

✗ No security guard present.

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

✓ A security guard should be employed to monitor who is entering or leaving the building and be present in case of any unwanted visitors coming to the premises.

7. Entrance and Exit

✗ I entered the industrial unit through a large door used to load completed sheds. If the same door which is used for loading deliveries is used for entrance/exit, it will be very difficult to keep track of who has entered or left. Therefore, a hacker could easily enter the building and obtain sensitive information from the company.

✓ A separate entrance for visitors and for loading of deliveries. This may not be possible due to the company being situated in a small industrial estate.

Procedural Controls

Guidelines or agreements that require or advise people to act in certain ways with the goal of protecting information assets.

1. Protection of Information

✗ According to the Minimum Cyber Security Standard, sensitive information held by the company (such as customer’s personal and payment information) must be identified and catalogued. The company has not done this. GDPR policy has not been mentioned.

✓ The company must be clear about what, where and why they are holding sensitive information. The impact of the loss of information, its compromise or disclosure should be identified. There must be clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services. The company should follow the Computer Misuse Act of 1990 and the General Data Protection Regulations (GDPR) as well as other relevant laws.

2. Backup

✗ No backup strategy. Backup is essential as it prevents loss of information due to human error. A fault in the systems can also cause loss of information.

✓Identify and utilise a backup strategy.

3. Responsibilities of Manager

According to the Minimum Cyber Security Standard, appropriate management policies and processes should be in place to direct the overall approach to cyber security. The manager should make sure that departments understand and manage security issues that arise because of dependencies on external suppliers or through their supply chain in order to prevent supply chain attack.

4. Cyber Awareness

✗ One of the employees of the company was asked about what phishing is but they did not know the answer. “Phishing is a method of trying to gather personal information using deceptive e-mails and websites”.[2] If employees are not aware of this technique of stealing data, they could easily fall into the trap of hackers. This would then lead to personal and business information being stolen.

[2] https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

✓ The employees need to be trained on different forms of cyber security attack and safe browsing. This is essential in preventing infection of systems with malware and ransomware and stopping hackers from accessing sensitive information.

✓ Senior accountable individuals should receive appropriate training and guidance on cyber security and risk management and should promote a culture of awareness and education about cyber security across the Department.

Technical Controls

Suggested controls or countermeasures that use technology-based contrivances to protect information systems from harm.

1. Secure Access

1.1. Passwords

✗ The password of the user account must not be “guest” as this is not secure. Avoid use of generic IDs. It is highly essential that the company sets guidelines with regards to passwords otherwise it will be very easier for hackers to access computers and systems.

✓ Each visitor needs to have a specific username and password (containing a combination of lowercase and uppercase letters, numbers and special characters) generated for single use.

✓ The company should have password policies (a low-cost security measure). By enforcing password history, old passwords cannot be reused, and must be changed every few months. A minimum password length should be set, and passwords must have acceptable complexity.

1.2. Using PCs

✗ The PC was on and unlocked. Anyone can access information.

✓ PCs should be locked and a password is required to use them. Only users who are authorized should be provided access and not anyone who enters the company.

1.3. Revoking Access

When an employee leaves the organisation, their access to the company systems should be removed. This is because disgruntled employees can cause the company harm by abusing their access to the computers and information.

2. Permissions for Downloading Software

✗ I was able to install software as a guest. Downloading unauthorized and unlicensed software poses a serious security risk.

✓ Permissions must be set so that only a small number of employees who are authorized such as IT management personnel can install software.

3. Permissions for Accessing Files

✗ Apart from the finance and personnel folders, I could copy and read anything on the file server. This makes stealing of files and data very easy for hackers. Accidental human interference could lead to loss of data if files have not been backed up properly.

✓ Permissions must be applied to users as well as files.

4. Dubious Websites

✗ As a test of cyber security, I was able to access some dubious websites on the company PC. Many of these websites contain harmful software such as malware and viruses which can lead to employee and company details being stolen or computers within the company becoming infected.

✓ Dubious websites must be blocked.

5. Network Security Controls

5.1. Antivirus, Antimalware

Antivirus and antimalware software should be regularly updated. The business should pay for a subscription to an antivirus programme. It is essential for them to be running the latest versions of the antivirus software to prevent infection with malware or viruses.

5.2. Firewall

✗ The company is not using a firewall. Firewall is required as it establishes a barrier between the trusted internal network and the untrusted external network (the Internet).

✓ Use firewall which is configured properly with good DDoS mitigation.

5.3. Encryption

Disk encryption is another method which helps to protect information. Full disks and also files can be encrypted.

5.4. Remote Desktop Protocol (RDP)

✗ RDP should not be open as it leaves the system vulnerable to access by unauthorized people who can hack the system by getting administration rights.

✓ Check and fix issues with commonly hacked ports (including RDP) in security tests.

5.5. Removable Media

✗ The fact that a USB stick could easily be plugged in to copy information is very risky.

✓ A USB security management system must be implemented. USBs can spread infected files such as ransomware. In addition to this, “disgruntled employees can easily steal data using USB drives” and “a single flash drive can collapse an entire network if managed improperly.”[3] As an example, “IBM banned removable storage devices to encourage employees to use the company's internal file-sharing system.”[4]

5.6. Switch

✗ Avoid use of consumer grade switch.

✓A small business network switch should be used instead which is more flexible and secure.

[3] https://blogs.manageengine.com/desktop-mobile/desktopcentral/2017/04/12/6-reasons-enterprises-need-to-implement-a-usb-security-management-system.html

[4] https://searchsecurity.techtarget.com/answer/Removable-storage-devices-Why-are-companies-banning-them

5.7. Data Line

✗ Single data line. If line goes down, the company will no longer have internet access.

✓ More than one data line.

5.8. Company Laptops

✗ The sales team have been given laptops which connect wirelessly when they are in the office and to any connection they can find when they are travelling. Customer and business information is at risk as no VPN used.

✓ Equip laptops with VPN. It is best to avoid using any public Wi-Fi and instead use tethering.

5.9. Two-factor Authentication or 2FA

A significantly more robust security solution compared to passwords. It requires a one-time code. An authenticator app such as Google Authenticator is more secure than SMS. Token authentication can also be used but is expensive to distribute to all employees.

The website below provides a list of different companies offering 2FA solutions with quotes:

https://www.g2.com/categories/multi-factor-authentication-mfa

5.10. Authentication

Transaction authentication can be used which compares the user’s characteristics with what is known about them. For example, the company can check if the IP address of the customer matches the location where they should be. Computer Recognition Authentication is used to verify the user’s identity by checking the device they are using via installing a software plug on the user’s computer the first time they sign it. This is also a beneficial technique and keeps track of which devices the user is using to login.

5.11. CAPTCHAs

CAPTCHAs neutralize threats from hackers. The businesses can use CAPTCHAs as part of their login systems to create one more barrier to automated hacking systems. They are not easy to use for everyone, especially those who are visually impaired.

Kerberos and SSL/TLS are also used for authentication. SSL is essential because users who access the company website can see if the certificate is valid. The SSL/TLS support is built into all major browsers, so it is easy and inexpensive to implement and does not require special software.

Conclusion

Time is money, and a cyber attack could cost the company much more than the cost required to implement relevant techniques to prevent it and take a considerable amount of time to fix.