Project overview for portfolio upload

Project Title: Case Study: Information Security Proposal

Project Description :

The following project is a case study where I was acting as an Information Security consultant who had been recruited by the directors of a company whereby, I was required to recommend a security proposal. This proposal had to contain a suitable Information Security programme and a corresponding set of information security policies that this fictitious company could adopt.

Areas which were covered in this project are:

- Acceptable Use Policy
- Access Control Policy
- BYOD (Bring Your Own Device Policy)
- Risk & Incident Repones
- T Security
- Recommendations for an IT team
    - Directors' computer access
    - Domain Controller
    - OS Updates
    - Guest Network

Grade: A

Appendices have been removed to avoid plagiarism from future students, however I am happy to provide additional information or discuss the work further if desired.

Introduction

North GenOne, a Hydro Electricity company, was recently acquired by ReNewABC. ReNewABC identified the need for increased information security within North GenOne. This need was furthered on by recent events, in which, North GenOne's director was a victim of a ransomware attack by clicking a link in a phishing email. Therefore, the IT Manager (Sue Perkins) has now requested for a proposal to be developed that includes security policy and training to help North GenOne meet the security standard required by ReNewABC and to help recover from the most recent attack.

Background

Information security programs are developed for businesses to mitigate the risks of information security. These programs are often large and will provide extensive information such as a full risk assessment, policies, training & auditing. In order to ensure this proposal is concise, relevant and beneficial to North GenOne, security policies, relevant training & IT upgrade recommendations are the focus.

To ensure the following policies are comprehensive, allowing for North GenOne to effectively increase security, each policy will be designed through amalgamating the details of other relative policies, strengthening the rationale of each policy. Policy formatting & headings are derived from SANS information security policy templates (SANS, 2022). Suggested training is also included within the policy as part of the compliance section. This will allow training to be centred around each policy, with consideration given to how it will affect each department of North GenOne on & off site.

With concrete policy, regular training and a company wide ethos for continuous development, it should be an essential goal for each company to obtain ISO's to indicate a high level of information security for customers and minimise risk across the board though this way of operating.

Recommendations - Policies & Training

1. Acceptable Use

1.1. Overview

North GenOne's Acceptable Use Policy (AUP) aims to protect company information, employees and customers by outlining essential foundation rules that employees will abide by before gaining access to company systems. This AUP is applied company wide & will avoid technical language where possible, ensuring universal understanding regardless of technical literacy, a problem of the previous AUP.

1.2 Purpose

Informing employees of their obligation to the secure use of North GenOne's technology. Due to the recent ransomware attack faced by North GenOne this AUP is security centred.

1.2.1 Employees are not permitted to discuss sensitive information involving North GenOne outside of the company premises.

1.2.2 Employees will not discuss North GenOne information to non-employees.

1.2.3 All employees must ensure sensitive information is stored only within the North GenOne, unless given explicit permission by a manager to do so. Managers must sign off on all work leaving the premises.

1.2.4 Certain websites will be blocked on company devices to ensure browsing is safe and regulated for employees.

1.2.5 Employees will not use company property for any business venture outside of the North GenOne.

1.3 Implementation

This AUP will be implemented across the entirety of North GenOne. This policy is fundamental and as a result will require all offsite workers to attend in person. Through attending in person this will allow for the policy to be introduced through role based training. Each department will take part and will work through all the potential violations of the AUP that a specific department might encounter, such as a breaking of GDPR regulation in the admin department. This type of involved training will happen around once a year to ensure a consistent refresh. It is essential for all employees to attend.

2. Access Control

2.1. Overview

North GenOne has a number of staff both on and off site with varying roles & level of authority. Currently, there are no security protocols in place to monitor the accessibility of resources across the business. Sue Perkins has detailed there is a possibility for any employee to access sensitive data & crucial functionality of North GenOne from any level of the business. This can lead to employees knowingly (or unknowingly) tampering with or sharing sensitive information about North GenOnes customers and creating issues for functionality of the operational technology.

2.2 Purpose

2.2.1 Define remote working requirements for all workers under NorthGenOnes employment to ensure all remote and on-site work is done securely.

2.2.2 For off-site workers this policy will include the use of VPN’s to ensure a private, encrypted connection when working with company data and operations.

2.2.3 Remote access software must be regularly updated to ensure it is on the latest version.

2.2.4 Both onsite & offsite workers will adhere to a strict password creation policy that will ensure all passwords created by employees will meet a specific minimum requirement such as minimum of 16 characters (SANS, 2023)

2.2.5 This is accompanied by Multi-Factor Authentication requirements on all systems, including operational technology (SCADA & PLC) and business management software such as the ERP system

2.2.6 Additional security controls will reduce accidental crossover and information spillage that was happening in North GenOne as a result of no access controls.

2.2.7 Creating additional walls of security to provide additional time for the company to react and implement an Incident response plan that will be highlighted further in the proposal.

2.3 Implementation

Regular training is essential for implementing this policy across North Gen One. Targeted training for different departments will be necessary in this situation. For example, off-site workers should receive regular training on the installation and upkeep of a VPN to ensure that it is regularly maintained to provide a strong connection into North GenOne's operational security (NCSC, 2023). This education on managing VPNs should be packaged together with additional security for access control, including features such as Multi Factor Authentication training. MFA training can be given company wide and together with VPN training should be given in company onboarding and again every six months to keep on top of the latest breaches & exploits. This training will be executed through a supervised walkthrough by an IT manager to ensure each employee knows how to install, set up and manage their VPN, MFA and passwords as these are crucial security functions that require clear direction from management.

3. BYOD (Bring Your Own Device)

3.1 Overview

North GenOne employees are largely in favour of bringing their personal devices to the workplace to use during work hours and on the work network. Sue Perkins has made assurances that this is only an occurrence during break and lunch hours - not interfering with work - however this is most likely incorrect. Regardless of the time in which employees use these devices, by simply having them in the workplace, or on the network and with no safety measures introduced it leaves North GenOne very vulnerable for data breaches (NCSC, 2022). There is a recognised worry for resistance from employees when implementing BYOD, therefore it is important that the policy introduces restrictions in a gradual but effective manner. This resistance will be mitigated by not focusing on any of the deployment strategies such as Mobile Device Management (MDM) or Mobile Application Management (MAM) as they are too intrusive for the current attitude towards BYOD in North Gen One.

3.2 Purpose

3.2.1 To create some network segmentation between BYOD devices & North GenOne devices. This will provide additional benefit of a network segmentation between visitor devices & North GenOne Devices.

3.2.2 To ensure no company software or information is stored on personal devices .

3.2.3 That clear definitions over how a BYOD device is defined and how this usage will look in the office for employees. This will also apply to how BYOD will be applicable to offsite workers.

3.2.4 Ensuring BYOD devices are used only during break & lunch, and that they are used in locations where NorthGen work is not taking place.

3.2.5 Removal of BYOD device if BYOD policy is knowingly breached.

3.2.6 Further discipline if BYOD policy is continuously violated.

3.3 *Implementation*

Due to the resistance towards BYOD policy within North GenOne it is important to deliver training in a way that will allow employees to get on board with the new policy. This will be done through interactive training sessions where the staff members can openly ask questions regarding their device usage under the new policy. There also should be a margin of error for the first 6 months to account for the adaptability curve some might have in reducing personal usage. Over time it is important to begin developing a stricter BYOD policy for new starts, this can be done by implementing Mobile Device Management where employees are given personal devices that have company software pre installed to help with safe browsing and correct usage.

4.1 Risk & Incident Response

4.2 Overview

After falling victim to the ransomware attack North GenOne did not have an incident response plan in place to help combat this security breach. Therefore an incident response plan should be developed to identify potential risks that the business will face and to develop plans that mitigate these risks if a future breach were to happen. Therefore, through performing regular risk assessments, North GenOne will aim to identify potential attacks ahead of time. As a result of no incident response plan, the directors of the company ultimately paid the ransom for their files to be returned in order to ensure that business could resume. Had a detailed incident response plan be drafted, this could have been avoided. This policy will encourage North GenOne to draft both a disaster recovery & a business continuity plan in the event that this type of breach takes place once again.

4.3 Purpose

4.3.1 Risk Management; Factors of risk outlined, categorised and a mitigation plan put into place by directors to try and meet.

4.3.2. Creation of a business continuity plan. This plan will focus on how the Operational Technology, which controls the main operations for North GenOne will stay operational in the event of a breach.

4.3.3 Continuity of business operation is allocated as a top priority for North GenOne, above all other assurances.

4.3.4. A disaster recovery plan will be created to ensure there are measures in place so that employees know, in the event of a large outage, how to ensure that its systems will become functional again.

4.4 Implementation

Regular training across the company will ensure that all employees within the business know the emergency proceedings should a breach take place. This training can be structured around running mock breaches or operational downtime scenarios where employees can role play to help learn their activity in as much detail as possible. This training should be often and at an increased frequency when there is an influx of new customers or employees as these variables are hard to account for until it happens.

5.1 IT Security

5.2 Overview

As a result of the encouragement from ReNewABC and the most recent ransomware attack, North GenOne realises the need for change around its information security. The ethos of trust throughout the company has meant many fail to maintain essential, basic level security protocols such as setting up MFA, choosing a good password and encrypting data. Therefore it is important to introduce a policy that focuses on the IT implementation of security. By taking a proactive approach to its information Security, North Gen One is aiming to stay ahead of other potential breaches. North GenOne can do this by implementing anti virus on all systems, using correct malware detection software, updating legacy systems and carrying out security audits to ensure there is sufficient security implemented.

5.3 Purpose

5.3.1 Determine the best suited anti virus software to install on all company devices and ensure each system is equipped with this.

5.3.2 Developing a malware detection technique to provide documentation, providing a foundation for an incident response plan.

5.3.3 No legacy systems should exist, updates should be downloaded and installed when possible to avoid exploitable software.

5.3.4 Security information given out to every new start in the onboarding process to create a new ethos throughout the company.

5.4 Implementation

In response to the recent ransomware attack faced by the directors, it is important that they lead by example when implementing training for malware & security breaches. Firstly, a baseline of knowledge of security attacks should be defined throughout the company. This is achieved through the NCSC's E-learning that is focused on information security and best practice (NCSC, 2021). Every current employee will undergo this learning. It should also be a section of North GenOne's onboarding process.

Security audits are extremely valuable to a company. North GenOne will not have any experienced security professionals for a while therefore ensuring someone coming in with a plethora of experience who can provide guidance for keeping security controls up to date through security auditing is essential. To increase the IT professionals' security knowledge within the business, SANS offers a wide variety of relative in depth courses that would be beneficial for the IT team to consider (SANS, 2023).

Recommendations - IT

It is understood that North GenOne are aiming to update their systems across the coming year once security policy & principle has been implemented across the board. However, due to the recent ransomware attack, and the current situation regarding some crucial operational technology it is essential there is some immediate change to ensure information security.

Directors Computer

Sue Perkins has stated that there is no longer ransomware active on the machine that was infected and that after the ransom was paid the ransomware was removed. Whilst this might seem to be the case, ransomware can often lay dormant on a machine and is able to be reset by the malicious actor (Exabeam, 2022) . It is important that the director's machine be replaced swiftly to ensure that no more damage is done. This is preferable to a digital forensics investigation due to the lack of security knowledge within North GenOne to ensure this is done correctly as oftentimes these attacks can be difficult to fully remove.

Domain Controller

North GenOne’s domain controller is running Windows 2012 which has just recently stopped receiving support as of October 30th 2023 (Nakarnam, 2023). Unsupported software is a target for hackers so therefore ensuring the domain controller is updated and on a secure version of Windows Server (2022 is the latest) will be paramount. This is an upgrade that should be of a high importance to North GenOne due to the high importance of the functionality of the domain controller controlling authorisation on servers.

Operating System Updates

When looking at CVE Details, an online security vulnerability database, we can see an alarming amount of reported exploits for Windows 7 and even greater for Windows XP (CVE, 2013). Windows 7 is currently being run by; Onsite Manager, one IT Technician (another is on Windows XP) and each Offsite Operator of the Operational Technology. This is a simple update that will tighten the North GenOne's security both onsite & for the Operational Technology.

Guest Network

Creating a separate guest network at North GenOne is suitable two fold, firstly it will allow visitors to join a network isolated from the operational technology in the business. Secondly, it can enable employees to use their own devices, separating their device usage from the main network of North GenOne. This can also reduce the risk of breaching the BYOD policy that is being suggested. This will provide additional security as opposed to simply creating a password protected network. However, this is the more costly and time consuming option, therefore North GenOne may wish to wait till they see a broader implementation of security policies across the business.

Summary

In implementing all security policy, training and IT updates suggested, it puts North GenOne's information security in a very advantageous position. They will have a solid foundation of comprehensive policies, training and the technology to help implement robust information security. This will help move North GenOne forward in trying to achieve the ISO standard 27001 for Information Security. This is the gold standard for businesses as it is a widely recognised standard that will allow North Gen One to show its commitment to information security globally. Through constant training and adhering to the proposed policy North GenOne should be aiming to achieve this standard in a year.