# **Assessment Task 3: Network Security Proposal**

Contents

[**Assessment Task 3: Network Security Proposal** 1](#_Toc169079418)

[1. Security plan 2](#_Toc169079419)

[2. Important assets identified 3](#_Toc169079420)

[3. Risk assessment 3](#_Toc169079421)

[4. Security policies 5](#_Toc169079422)

[5. Physical security 6](#_Toc169079423)

[6. Contingency planning 7](#_Toc169079424)

[1. Incident Response Plan 7](#_Toc169079425)

[2. Disaster Recovery Plan 8](#_Toc169079426)

[7. Email to CIO 10](#_Toc169079427)

[8. Meeting with consultant 11](#_Toc169079428)

## Security plan

1. Monitor security posture: log reviews, vulnerability scans, and penetration tests.
2. Conduct security audits and compliance checks.
3. Incident response and disaster recovery: incident handling and business continuity planning.
4. Continuous improvement: update policies, and controls based on new threats, and periodic security reassessments.
5. Design security architecture and controls: Network security, host security, access controls and data security.
6. Implement technical security controls.
7. Deploy security awareness training.

End

1. Identify assets (data, hardware, software, facilities, people.
2. Perform risk assessment: Identify threats and vulnerabilities, analyse potential impacts, and calculate risk levels.
3. Determine security requirements and objectives.
4. Develop security policies and procedures.

* Allocate resources and budget

Managing Phase

Planning Phase

Building Phase

Start

## Important assets identified

1. Building Assets

* Head office building in Brisbane
* Branch office building in Cairns

1. Hardware Assets

* Servers (DC Servers, Collaboration Server, VoIP, DHCP Server, Monitoring Server, Web server, HR database, file servers for marketing and customer service)
* Desktop PCs and laptops
* Network equipment (switches, routers, firewalls, Access Points)
* Telephony systems (IP Phones)

1. People Assets

* Executives and top management
* IT staff
* Customer service representatives handling sensitive customer data
* Human resources staff with access to employee records
* Marketing staff with access to strategic plans and materials

## Risk assessment

|  |  |  |  |
| --- | --- | --- | --- |
| Likelihood | Impact | | |
| Low | Medium | High |
| Low | Low | Low | Medium |
| Medium | Low | Medium | High |
| High | Medium | High | High |

**Table 1. Risk Assessment**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No. | Threat | Vulnerability | Control | Likelihood | Impact | Risk Rating |
| 1. | Data Breach | Outdated Firewall, Weak Passwords | Firewall Upgrade, Strong Password Policy, Multi-factor Authentication (MFA) | High (5) | High (5) | High (25) |
| 2. | Malware Infection | Lack of Endpoint Security, Susceptible to Phishing Attacks | Deploy advanced endpoint protection, automated patch management, email filtering/scanning | Medium (3) | Medium (5) | High (15) |
| 3. | Denial of Service Attack | Unprotected Network Infrastructure, Reliance on a Single ISP | Implement Intrusion Detection/Prevention System (IDS/IPS), Network Traffic Monitoring, Redundant ISP | Medium (3) | Medium (3) | Medium (9) |
| 4. | Insider Threat | Lack of Access Control, Inadequate Data Handling Procedures, Weak Employee Onboarding/Offboarding Processes | Implement Role-Based Access Control, Data Loss Prevention (DLP), Employee Background Checks, Security Awareness Training | Low (1) | High (5) | Low (5) |
| 5. | Physical Theft/Damage | Inadequate Physical Security Controls at Both Offices, Lack of Environmental Monitoring in Server Rooms | Implement Access Control Systems, Surveillance Cameras, and Environmental Monitoring | Medium (3) | Medium (3) | Medium (9) |

1. **Threat:** Hackers or malicious actors attempting to gain unauthorised access to Helpyou's network and steal sensitive customer data. **Vulnerability:** Helpyou's outdated firewall may not effectively block the latest threats. Weak password practices increase the risk of brute-force attacks.  
   **Control:** Firewall Upgrade, Strong Password Policy, Multi-factor Authentication (MFA). **Impact:** Data breaches can result in financial losses (regulatory fines, lawsuits), reputational damage, loss of customer trust, and operational disruption.
2. **Threat:** Malicious software designed to disrupt systems, steal data, or gain unauthorised access. **Vulnerability:** The lack of comprehensive endpoint security leaves workstations vulnerable. Employees clicking on phishing links in emails is a common entry point.  
   **Control:** Deploy advanced endpoint protection, automated patch management, email filtering/scanning. **Impact:** Malware can cause data loss, system downtime, and financial losses from fraud, and require significant resources for remediation.
3. **Threat:** Attacks designed to overwhelm Helpyou's network or servers with traffic, making them unavailable to legitimate users. **Vulnerability:** An unprotected network infrastructure is susceptible to DoS attacks. Reliance on a single ISP creates a single point of failure.  
   **Control:** Implement Intrusion Detection/Prevention System (IDS/IPS), Network Traffic Monitoring, Redundant ISP. **Impact:** DoS attacks can disrupt business operations, lead to financial losses due to downtime, and damage customer relationships.
4. **Threat:** Malicious or negligent actions by employees, contractors, or authorised users with access to Helpyou's systems and data. **Vulnerability:** Lack of access controls, inadequate data handling procedures, and weak onboarding/offboarding processes increase the risk of insider threats. **Control:** Implement Role-Based Access Control, Data Loss Prevention (DLP), Employee Background Checks, Security Awareness Training. **Impact:** Insider threats can lead to data theft, sabotage, financial fraud, and reputational damage.
5. **Threat:** Unauthorised individuals gaining physical access to offices or server rooms to steal hardware or cause damage and environmental factors (fire, flood) disrupting operations. **Vulnerability:** Inadequate physical security measures at both offices leave Helpyou vulnerable to theft and vandalism. Server rooms require enhanced environmental controls. **Control:** Implement Access Control Systems, Surveillance Cameras, and Environmental Monitoring. **Impact:** Loss of valuable hardware, data loss if backups are compromised, downtime, and business disruption.

## Security policies

1. **Title:** Password Protection Policy  
   **Purpose**: To establish requirements for strong passwords that are difficult to guess or crack, protecting against unauthorised access.  
   **Scope:** This policy applies to all Helpyou employees, contractors, and anyone with access to company systems and data.  
   **Security rules:**

* Passwords must be at least 12 characters long and include a mix of upper and lowercase letters, numbers, and special characters. Avoid using dictionary words or personal information.
* Passwords must be changed every 90 days, and the previous 10 passwords cannot be reused.
* Default vendor passwords must be changed immediately.

1. **Title:** Information Logging Standard  
   **Purpose**: To ensure logging of system events for security monitoring, incident response, and compliance.  
   **Scope:** Covers all Helpyou information systems, servers, network devices, and applications.  
   **Security rules:**

* Enable logging on all systems and devices.
* Log user activities like logins, file access, and security violations.
* Keep logs for at least 1 year.
* Review logs regularly for any suspicious activity.
* Ensure the integrity and confidentiality of log data.
* Strictly control access to the logs.

1. **Title:** Email Policy  
   **Purpose**: To outline the acceptable use of Helpyou’s email system and prevent security incidents.  
   **Scope:** This applies to all employees and anyone using Helpyou’s email services.  
   **Security rules:**

* No sending unauthorised business data or offensive content.
* Do not open suspicious emails/attachments from unknown sources.
* Use email encryption for sensitive information.
* Avoid using email for transferring large files.
* Email auto-forwarding to external accounts is prohibited.
* Company email can be monitored for compliance.

1. **Title:** Internet Usage Policy  
   **Purpose**: To manage risks from internet usage and protect Helpyou’s network and systems.  
   **Scope:** Covers all Helpyou employees, contractors, and guests accessing the internet.  
   **Security rules:**

* No accessing inappropriate, illegal, or offensive websites.
* Downloads must be scanned for malware before use.
* Unauthorised software downloads are prohibited.
* Internet usage may be monitored for compliance.
* Limited personal internet use is permitted if it doesn't impact work.

1. **Title:** Router and Switch Security Policy  
   **Purpose**: To secure Helpyou’s network infrastructure from threats and unauthorised access.  
   **Scope:** Applies to all network devices like routers, switches, firewalls, and wireless access points.  
   **Security rules:**

* Change all default passwords and disable unnecessary services.
* Enable secure management access (SSH, HTTPS).
* Configure role-based access controls.
* Implement secure network segmentation and zoning.
* Regularly apply software patches and updates.
* Enable logging and monitoring of network devices.

## Physical security

**External Perimeter Defences**

* Install perimeter fencing or barriers around the office buildings to control access.
* Deploy exterior lighting and security cameras to monitor the premises.
* Implement access control systems like card readers at entry/exit points.
* Have a manned security guard station at the main entrance.

**Internal Physical Security**

* Secure the server rooms with reinforced doors, locks, and access controls.
* Install interior security cameras to monitor sensitive areas like server rooms.
* Implement motion sensors and alarms in restricted areas.
* Use locked cabinets or cages to store critical hardware like servers.
* Enforce strict key/access card management and visitor logging procedures.

**Hardware Security**

* Use cable locks to secure desktop PCs, laptops, and other portable devices.
* Enable hard disk encryption and BIOS/firmware passwords on systems.
* Implement secure asset disposal procedures for retiring old hardware.
* Install environmental monitoring (temperature, humidity, fire detection) in server rooms.
* Deploy uninterruptible power supplies (UPS) and backup generators for critical systems.

## Contingency planning

### Incident Response Plan

**Preparation Phase**

* Establish an incident response team with defined roles and responsibilities.
* Develop detailed incident response procedures and communication plan.
* Provision of the tools and resources needed, such as forensic workstations and malware analysis tools.
* Conduct security awareness training for all employees.
* Test and update the incident response plan regularly.

**Identification Phase**

* Continuously monitor systems for security incidents using SIEM, IDS/IPS, antivirus, etc.
* Analyse alerts and logs for signs of compromise.
* Have a hotline for employees to report suspected incidents.
* Define criteria and data sources to verify an incident has occurred.

**Containment Phase**

* Quickly isolate/disconnect affected systems to prevent further damage.
* Change passwords and revoke access for compromised accounts.
* Block malicious IPs, domains, and communication channels at firewalls.
* Capture volatile data from affected systems for forensic analysis.

**Eradication Phase**

* Identify and remove malware, rootkits, backdoors from all affected systems.
* Correct system misconfigurations that allowed the incident to occur.
* Conduct detailed forensic analysis to determine the root cause.
* Remediate all vulnerabilities that were exploited.

**Recovery Phase**

* Restore systems and data from trusted backups once eradication is complete.
* Patch vulnerabilities and harden systems with the latest security updates.
* Monitor for any signs of reinfection or recurring incidents.
* Allow normal operations to resume once recovery is verified.

**Lessons Learned Phase**

* Perform a detailed analysis of the incident.
* Update incident response plans based on lessons learned.
* Implement additional security controls to prevent similar incidents.
* Share information to improve overall security posture.

### Disaster Recovery Plan

**Backup Method**

* Use enterprise-grade backup software like Veeam or Commvault to back up the database server.
* Leverage snapshot and replication technologies for quick backups with minimal impact.

**Backup Types**

* Perform full backups of the database server weekly.
* Perform incremental backups daily to capture changes since the last full backup.
* Maintain a rolling window of 2 weeks' worth of daily incremental.

**Backup Schedule**

* Full backups every Saturday at 2 AM.
* Incremental backups daily at 10 PM.

**Backup Storage**

* Back up to a local disk storage for fast restores.
* Replicate backups to an off-site location or cloud storage for disaster recovery.
* Encrypt backups in transit and at rest using industry-standard encryption.
* Rotate and retire older backup media regularly based on the retention policy.

**Data Restoration Procedures**

* Identify the most recent known full backup to use as the baseline.
* Stage the full backup in a restoration staging area.
* Apply incremental backups in chronological order on top of the full backup.
* Perform integrity checks on the restored data before putting it into production.
* If data is corrupted, go back to the previous known full backup.
* Redirect database services to the restored server once verified.
* Monitor and test the restored server before allowing full production access.

## Email to CIO

Dear CIO,

As requested, I have developed a comprehensive security plan to upgrade Helpyou’s existing security posture and address the identified risks and vulnerabilities. The plan includes the following components:

* + - 1. Security Plan Phases

A flowchart outlining the key activities in the planning, building, and managing phases for implementing robust security controls.

* + - 1. Asset Identification

Critical building, hardware, and people assets requiring protection have been identified.

* + - 1. Risk Assessment

A table listing 5 major threat types, associated vulnerabilities, likelihood, impact, and risk ratings. Detailed assessment of each threat, including control measures and potential business impacts.

* + - 1. Security Policies

Clearly defined policies for passwords, logging, email usage, internet access, and network equipment security.

Policies cover the purpose, scope, and specific security rules to be enforced.

* + - 1. Physical Security Plan

Multilayered physical controls for external perimeter, internal areas, and hardware safeguards.

* + - 1. Contingency Planning

Detailed incident response plan with 6 phases for effective incident handling. Comprehensive disaster recovery plan focusing on backup strategies and restoration procedures.

I would greatly appreciate it if you could review the attached documents and provide your feedback or any additional requirements. Implementing this security program is crucial for protecting Helpyou’s assets and mitigating risks as we expand operations.

Please let me know if you need any clarification or have additional concerns to be addressed. I look forward to discussing this further.

Thank you,

Thong Thao

IT Security Consultant

## Meeting with consultant

*8. Group Discussion.MP3*