# ICT380

## Assignment 2

# “Vanderlay Industries”
# Security Master Plan


## Chris Cigana (33605148)

# Table of Contents.

# Table of Contents

## Abstract

An information security program is a document that illustrates an organisations information security vision, strategies, goals, programs and processes [Giles, 2009]. It is developed and used to provide guidance to the organisations direction and development in the information security domain. Inside the Security Masterplan, the organization provides a detailed outline of the risks and the mitigation plans that need to be developed and how team members can provide depth and consistent to the overall information security framework. The program is the result of extensive planning which occurred over almost 10 weeks and was structured and conducted around the key leadership roles within the organization. The principles around which the information security policy of Vanderlay Industries revolves is centered on the "6 P's", these being: Planning; Policy; Programs; Protection; People; and Projects.

To create and develop the information security program for Vanderlay Industries, we adhered to a 10-step process that enabled us to define and focus our efforts on the key areas of the program and how it relates to the organization. These steps include: Establishing information security teams; Manage and inventory information assets; Decide on regulatory compliance and standards; assess threats, vulnerabilities and risks; Manage risks; Create and incident management and disaster recovery plan; Manage third parties; Implement security controls; Conduct SETA programs.

## Establish Information Security Team Members:

The below staff members have been identified to be key stakeholders of the overall security posture of Vanderlay Industries, so it is suitable for them to become the members of the InfoSec team. They will become integral in the long-term success of the InfoSec program and their input and involvement are crucial. Periodic meetings and regular correspondence between security team members will progress the program and ensure the commitment and involvement of all key stakeholders.

CEO: Chris Cigana

Director (back office): Mohammed Ausanajali

CIO: Chris Cigana

CSO: Mohammed Ausanajali

Director (sales & product): Mohammed Ausanajali

Legal Officer: Chris Cigana

## Manage and Inventory Information Assets:

Extensive documentation of the organizational structure and daily operating environment of Vanderlay Industries was provided by the Company and was further refined through the key stakeholder interviews. The reason interviews were also conducted in addition to the written documentation is that the InfoSec team needed to hear where stakeholders thought the real security issues were located- not just what appears on a organizational spreadsheet.

The information assets that Vanderlay Industries own can be divided up into certain key areas, these areas and the assets they contain, are listed in detail below:

- Organisational Overview:
    - Developed software and hardware for the oil and gas industry.
    - Processing services that compute and analyse client information.
    - **Large $$$ sector**- importance of this fact to the organization cannot be overstated.
        - **Any organizational brand damage in the wider sector will have severe impacts on the business**.
    - Significant efforts already conducted to future-proof and implement automation organization wide.

- Monitoring Software: "SensorDrill" and "MeasureMe". Vanderlay software that monitor drilling and pumping.

- Services: Provide services in processing and interpreting collected seismic data using internally developed software (Shake and Quake)
    - These services must be of the highest possible quality in both professionalism and content of subject matter experts.
    - Vanderlay retains the software (Shake and Quake) and clients give us their data to process- we must maintain the CIA of their data during processes.

- Market Information:
    - Vanderlay holds 40% market share, closest competitor also holds 40%. Competitor offers same services and holds similar software.
    - Other 20% of market is held by smaller companies that offer one or the other of the services- not both.
    - Possible risks involving industrial espionage and theft of Vanderlay IP.

- Research and Development:
    - **Project 1**: R&D project, major upgrade to monitoring software expected for release in 6 months time.
        - Upgrade provides real time remote monitoring of drilling and pumping via satellite or landline.
            - Quality and consistency of data transmission and bandwidth a real issue that must be examined.
            - Software will be tested and upgraded with Beta test data and feedback.
        - Often requested- but this will be Industry First. In close Beta testing phase, larger clients will get opportunity to test once ready.
            - Industrial espionage a real possibility here, and significant protections must be in place for this eventuality.
            - Legal (NDAs and documentation all in place before clients use)
        - Expected to raise Vanderlay market share up an additional 10%.
            - Project considered Top Secret and must be handled accordingly.
            - Also- secrecy is essential until release date- will provide maximum impact for market share.
    - **Project 2**: Software that will increase speed of data processing through splitting workload to many different servers- upto 30% speed increase.

- Projected $30 mil increase annually, 12 months away from completion. Competitor working on something very similar.

## Results from Interviewing Key Stakeholders:

To further our planning and information gathering, we spent several weeks interviewing and brainstorming with the members of the InfoSec team. This was intended to provide some depth and context to the provided written documentation, and also give us insight into the day-to-day security posture and opinions of the InfoSec team members of where key failings lie and also where focus should be concentrated.

CEO:

- Industrial espionage.
    - Serious and impactful scenario that can cause long term damage to organization brand and profit bottom-line. Possible fix is to implement a form of vetting process for new employees/third-parties to help reduce risk profile.
    - Establishment of a well-trained and drilled incident response team to enable quick reaction to any possible security incidents.
- High staff turnover resulting in loss of company IP regarding InfoSec policy and infrastructure.
    - In-depth documentation of the policy and procedures relating to InfoSec introduction and education to all staff members. Establishing a baseline is part of a develop information security program which will help organization-wide.

CIO:

- Due to lack of mature security infrastructure, ICT services at high risk of compromise.
    - Establishment of InfoSec program will help overall organisational posture and development and implementation of incident response team will mitigate potential attacks.
- Business operations that are reliant of ICT infrastructure are not prepared for large-scale service disruption.
    - Design and development of planning and processes for ensuring business continuity and disaster recovery should the scenario ever occur.

CSO:

- Weak mobile device management results to security threats to the organisation's information systems.
    - Clearly defined policies on BYOD will help to remedy this.
- Time theft.
    - Implementation of organizational wide biometric systems will help track employee time and also help raise the security posture of the organization.

Director (sales & product):

- Weak procedures by employees in securing the organisations data and information systems in the context of day-to-day operations.
    - Stringent policy that tasks IT with protecting the organisations confidential and private data from sales reports to employee social security numbers.

Legal Officer:

- Legal and regulatory level compliance.
    - Periodic checks and balance against any industrial regulations that our organization may fall under need to be implemented and monitored through the company. Strict processes regarding responding to regulatory breaches will mitigate long-term damage done to the organization.
- Misuse of company technical property by existing employees or third-party vendors.
    - Extensive development of ISSP's and SysSP's will allow for large-scale regulation and expectation management of all resources inside the organization.
    - SETA program will keep staff informed and educated on the risks and possible consequences of property misuse.
    - Documentation will allow for disciplinary action to occur if breached.

## Assess Threats, Vulnerabilities, and Risks & Security Implementation to Mitigate these Threats, Vulnerabilities, and Risks:

The below assessment of the threats, vulnerabilities and risks that are relevant to Vanderlay Industries is to be examined and analysed in addition to the key stakeholder threats, vulnerabilities, and risks that were identified in the interview process. This is followed by a Threat Vulnerability Analysis (TVA).

Company Overview:

- Due to high $$$ value of oil and gas industry, any small damage or detrimental affect to organizational brand or reputation will have severe and long-lasting affects.
- Due to focus on long-term future-proofing and automation, Vanderlay may lose oversight of day-to-day operations and may become complacent.

Monitoring Software:

- (SensorDrill and MeasureMe) Flagship products that need to succeed. Must be extensively designed, tested, and monitored and supported once in place with third-party.
- Licensed products, risk of negative feedback must be managed through in-depth and ongoing stakeholder engagement.

Services:

- These services must be of the highest possible quality in both professionalism and content of subject matter experts.
- The software, which is internally developed and supported, must be 1st class in both design and from a security viewpoint. Vanderlay will be judged in the software it outputs and licenses, so it must be as close to security proof as possible- this includes regularly testing and patching.
- Vanderlay retains the software (Shake and Quake) and clients give us their data to process- we must maintain the CIA of their data during processes.

Market Information:

- Due to "niche" industry, Vanderlay must remain proactive and dynamic to remain in control of their market share and to hopefully grow the business.

- Vanderlay holds 40% market share, closest competitor also holds 40%. Competitor offers same services and holds similar software.
- Other 20% of market is held by smaller companies that offer one or the other of the services- not both.
- Possible risks involving industrial espionage and theft of Vanderlay IP.
- Inside threat actors are also a high possibility and must be considered when discussing threats to market share.

Research & Development:

**Project 1**: R&D project, major upgrade to monitoring software expected for release in 6 months time.

- Upgrade provides real time remote monitoring of drilling and pumping via satellite or landline.
    - Quality and consistency of data transmission and bandwidth a real issue that must be examined.
    - Software will be tested and upgraded with Beta test data and feedback.
- Often requested- but this will be Industry First. In close Beta testing phase, larger clients will get opportunity to test once ready.
    - Industrial espionage a real possibility here, and significant protections must be in place for this eventuality.
    - Legal (NDAs and documentation all in place before clients use)
- Expected to raise Vanderlay market share up an additional 10%.
    - Project considered Top Secret and must be handled accordingly.
    - Also- secrecy is essential until release date- will provide maximum impact for market share.

**Project 2**: Software that will increase speed of data processing through splitting workload to many different servers- upto 30% speed increase.

- Projected $30 mil increase annually, 12 months away from completion. Competitor working on something very similar.
    - Legal documentation of the design and Alpha build must be stringent to ensure no litigation from organizational rival.
    - “The devil is in the details…”
- Competitor ahead of Vanderlay and expected to finish in 2 months.
    - Ensure legal process maintained and documented, Vanderlay’s professionalism and our long-term positioning with Project 1 will ensure we emerge the strongest organization in the long-term
- Project will involve infrastructure upgrade with additional network cables and upgrade of existing servers.
    - Physical security of Vanderlay assets become important with the increase of third-party contractors that will be hired for the upgrades. Possible vetting process for third-parties.
    - Speed must be maintained and by consistent for Vanderlay to keep marketing the difference. Ensure process is completed well- do not risk progress in order to keep up with competitor.
- Increased outlay in hardware to ensure software runs at peak efficiency.

- Process must be Project Managed effectively to ensure minimal cost overruns and delays to project.

Contractors and Vendors:

'Clean and Mean Pty Ltd':

- 2 cleaners officer hours, 4 cleaners after-hours.
  - Correct implementation of InfoSec policy will ensure limited opportunity for cleaners to "snoop around".
  - Vanderlay employees must be trained and regularly educated in InfoSec risks and counter-measures. (as pertinent for a SME)
  - CCTV monitoring of Vanderlay Office and Company areas after hours.

'Computex Pty Ltd':

- Provide network infrastructure- cable laying and network points.
- Work after-hours to minimize daily operations.
  - As with cleaners, strong InfoSec policies and procedures will minimise risk profile.
  - Regularly education and new employee on-boarding for InfoSec will maintain high standard.
  - Possible Vanderlay escort for sensitive areas that need to be upgraded.

'Printmaster Pty Ltd':

- Photocopier and printing suppliers and maintainers.
  - As above.

'PeopleRus Human Resources Pty Ltd':

- Employment agencies used by Vanderlay, used to provide permanent and temporary staff placements.
  - Possibly need to incorporate a vetting process at this level to rule out undesirable candidates early.
- Vanderlay used short-term contract staff extensively to meet temporary staffing requirements in various departments. Temp staff given same access to permanent.
  - Legal: stricter guidelines and organizational processes written up to dictate temp access and to improve overall segregation of sensitive areas and company IP.
  - InfoSec policy implemented that encompasses SysSP, etc
- Current employment situation is untenable and unsustainable, significant changes and improvements are needed in this space.

'Hungerbuster Pty Ltd':

- Vendor providing food and drink to vending machines and catering for functions etc.

Physical Security:

- The building and office environment are fairly secure, but need slight adjustments to ensure maximum security posture for the organization:
    - Ensure all visitors are escorted off premises once there business has concluded.
    - Swipe card access needs to be implemented for upper levels of building- especially sensitive areas such as IT infrastructure.
    - Swipe access needs to be implemented for building lifts, as they operate 24/7 and can be accessed by third-party vendors etc.

IT Infrastructure:

- Server Room:
    - Server room must remain locked at all times. IT staff will need swipe card access to gain entrance.
    - This precaution will reduce risk of insider threat actor, will also allow for loggin of who enters the server room and when.

- Wiring Closet:
    - Again, access to this room must be controlled and monitored.
    - Swipe card access needs to be implemented and third-party contractors need to be escorted through the building when working on this equipment.
    - Implementation of air-conditioning for this room is also a priority due to the large number of critical networking hardware that reside in the room.

- Data Processing:
    - The seismic data processing is run separate from the other organizational networks- this is good security practice.

IT Security:

- Client PC:
    - Process must be implemented to ensure that all Microsoft O/S and Outlook software are regularly patched as advised by MS. This must consider the compatibility issue already raised.
        - Despite the issue- security patching must occur, it greatly affects the security landscape of the organization.
        - Additional development work must be conducted on existing software to merge their compatibility with vendor products.
    - Departmental specific software and its installation must become a logged process to show data trails and operator usage.
    - Windows O/S must be upgraded from Windows 7 to Windows 10. Windows 7 is an outdated and obsolete piece of software that, traditionally, has produced a lot of software vulnerabilities.
    - Extensive register must be implemented to show what machines are running what O/S and what software etc. Especially as the R&D department as responsible for large ticket operations over the next few years. They must be trackable and monitored.
- Servers:
    - If resources allow, it would be prudent to merge the existing Domain controller servers and run one version, this would increase compatibility and the overall security of the system.

- The RAID 5 system is good enough for organizational needs, but consideration to upgrading may be necessary if the Projects are successful and more business acquired.
- Symantec software will need to be registered and updates conducted periodically or as required by the vendor.
- The IBM hardware will need to remain patched and secure, with obvious consideration to not affect existing information systems in the data processing functionality.

- IT Policies:
  - Discussed with information security policies and frameworks.
  - The EISP, ISSPs, and SysSPs will mitigate a lot of the risks that exist with weak or non-mature IT policies and practices.

**TVA:**

| Threat | Vulnerability | Asset and consciences | Risk | Solution |
|---|---|---|---|---|
| Outside actors gaining access to organizational IP to use for their own business ends. | Industrial espionage (high) | damage to organization brand and profit bottom-line | High<br>(losing a sensitive information ) | - a well-established Incident Response Team<br>- to implement a form of vetting process for new employees/third-parties to help reduce risk profile |
| Weak mobile device management | Cyber attacks | security threats to the organization's information systems. | High | defined policies on BYOD |
| High staff turnover | Compromising IP address of the InfoSec | loss of Company IP regarding InfoSec policy and infrastructure. | high | Strong and in-depth Documentation of the policy and procedures relating to InfoSec introduction and education to all staff members |
| Time theft. | security posture of the organization | Delay on many obligations of the company | Low | Implementation of organizational wide biometric systems.<br><br>Track employee time and raise the security posture of the organization. |
| Nature disaster flooding | Server room are on second floor | Unavailability of the server | low | Moving the server room to up floors |
| (DDos attack)<br>Denial of service | The configuration of firewall | Unavailability of websites | (High)<br>The downtime hours will cause a | A proper configuration and |

| | | | | |
|---|---|---|---|---|
| | | | potential loss of 6000$ per hour | monitoring of Firewall |
| Overheating in server room | Old Air condition | Most of the servers like emails, and websites won't be available for 5 hours | (High) Potential loss of 4000$ per hour | Purchase a new air condition |

## Principles of the Security Program:

Policy; Program Management; Risk Management; Life-cycle planning; Personnel/user issues; Preparing for contingencies and disasters; Computer Security Incident Handling; Awareness and Training; Security Considerations in Computer Support and Operations; Physical and Environmental Security; (Access Control) Identification and Authentication; Logical access control; Audit trails; and Cryptography.

Levels of controls:

- Management controls: cover security processes designed by strategic partners and performed by system administration.
- Operational controls deal with the operational functionality of security in the organization.
- Technical controls address tactical and technical implementations related to designing and implementing security in the Vanderlay Industries organization.

Defense in Depth:

- Implementation of security in layers.
- Requires that the Vanderlay organization established sufficient security controls and safeguards so that an intruder faces multiple layers of controls.

Security Perimeter:

- Point at which an organisation's security protection ends and the outside world beigns.
- Does not apply to internal attacks from employee threats or on-site physical attacks.

## Information Security Policy.

Information Security Policy, and the EISP that it is derived from, is the central cornerstone of every effective and efficient information security program and the quality and depth of an organisations security posture begins and ends with policy. Policies, such as ISSPs and SysSPs, are designed to define and provide structure in the workplace and explain and illustrate the overall will and vision of management. The information security policies for Vanderlay Industries will be tailored to the specific needs of the organization, based in part on the information we have gained about the structure and daily operations of the business.

There are three areas that need to be taken into consideration when developing information security policy, these are: the larger scale policies of the business; the networks that make up the business environment; the hardware and software systems that are being utilized by the organization; and the application systems that the business uses in the daily operations. By careful and detailed examination of the overall company policies, we can develop and implement effective and efficient information security policies.

The information security policies that have been developed by the Vanderlay Industries security program falls under three key categories: Enterprise Information Security (EISP); Issue-Specifc Security Policies (ISSP); and System-Specific Security Policies (SysSP). The EISP is the highest organizational level documentation, so they were developed first. Secondly the ISSP and SysSP were identified and developed, as was necessary in their individual contexts.

The individual policies that make up the information security program are attached in the Appendix section.

EISP:

- The enterprise information security policy is the high-level policy that sets the strategic direction, scope, and tone for all the organisation's security efforts (Whitman & Mattford, 2017). The EISP aligns closely with Vanderlay Industries missions and objectives and will aid in the shaping of the security philosophy for the company.
- The Vanderlay Industries EISP addresses compliance issues in two key areas: Ensure meeting requirements to establish program and responsibilities assigned to various organizational components; and use of specified penalties and disciplinary action.
- The information security program document is largely made up from the EISP and is populated by the EISP's key elements: Overview of corporate philosophy on security; Structure of the InfoSec organization and InfoSec team members; fully developed responsibilities for security that are shared by all members of the organization; fully articulated responsibilities for security that are unique to each role within the Vanderlay Industries organization.

ISSP:

- The issue-specific security policy is an organizational level policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a specific resource- such as a process or technology (Whitman & Mattford, 2017). The ISSP framework aims to protect both the employee and the organization form inefficiency and ambiguity.
- These policies require frequent review and updating, due to the rapidly changing IT environment. As new technology or business equipment is onboarded, the ISSP needs to be enlarged to encompass the new additions.
- The well-structured and developed ISSP's of Vanderlay Industries will accomplish the following: illustrate the companies expectations about how technology based resources will be utilized; provide documentation as to how the aforementioned resource is controlled and will identify access and authority to use; and indemnifies Vanderlay against liability.
- The information security program has utilized three approaches when creating and managing the ISSPs: created a number of independent ISSP document (Appendix 1); create a single comprehensive ISSP document (InfoSec Program); and create a modular ISSP document (EISP).

SysSP:

- The system-specific security policies of Vanderlay Industries function as standards and procedures to be used when configuring and maintaining systems. SysSPs can be divided into separate but equally important groups: managerial guidance; and technical specifications (Whitman & Mattford, 2017).

- The managerial guidance SysSP documents will guide and direct the implementation and configuration of technology and also address the organizational behaviour surrounding security of information.
- Technical specification SysSPs will be developed with input by the technical staff that will administer them in day-to-day operations. The SysSPs will illustrate the technical end-state of the software or hardware and provide a benchmark for the equipment to adhere to.
- An integral part if the technical specification of the SysSPs is the access control lists (ACLs). The ACLs of Vanderlay Industries will govern the rights and privileges of users and be comprised of user access lists, matrices, and capability tables.
- Vanderlay Industries will endeavor to develop both SysSPs and ISSPs concurrently, so that operational procedures and user guidelines will merge in scope and fundamentally improve the security posture of the organization.

## Incident Management and Disaster Recovery Planning:

A critical component of an effective and efficient information security program is an in-depth plan for incident management and disaster recovery. Incident response is fast becoming the key part of an organisations InfoSec posture, as threat actors are becoming more advanced and far more brazen- meaning that a security breach or incident is more likely than ever. How Vanderlay Industries responds to an incident or a disaster scenario is a crucial part of the strength of the information security program.

The Vanderlay organization will have a well-designed incident response program that involve the security team and other highly trained professionals who will be ready at a moments notice to step in an apply the organisations policies and procedures to mitigate all possible risks.

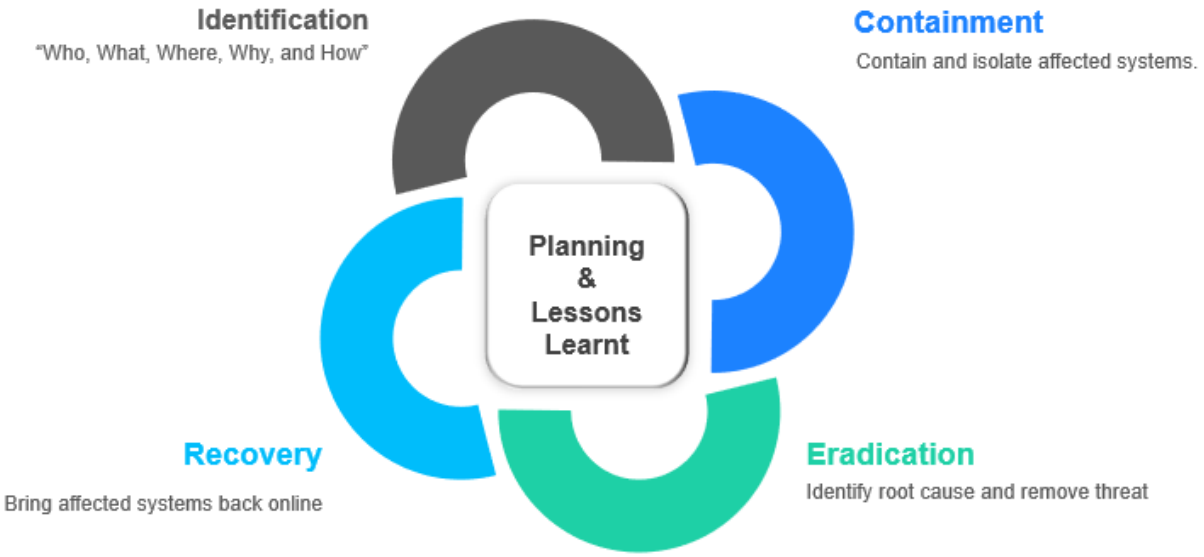
To effectively design this incident response plan, the security team must thoroughly understand the organisations priorities and demonstrate how to quickly take steps to contain any possible damage caused by a security incident. Fast and decisive action taken during this period will protect other elements of Vanderlay's network and information systems, thus helping to reduce the impact on the organization. The primary way the information security program will attempt to understand the threat landscape is by conducting a business impact analysis (BIA)

The main elements of the incident response plan are: senior management support; consistent testing; balance between detail and flexibility; clarification of communication channels; knowing who the organizational stakeholders are; emphasis on keeping the plan simple.

The methodology that will be employed by the incident response team once an incident has been identified are detailed below:

1. Preparation:
    a. This is the stage that outlines the plan in detail. The security team should review and define the underlying security policies that underpin the incident response framework. Team performs a risk assessment and prioritises potential issues. A communication plan is created and documentation prepared.
2. Identification:

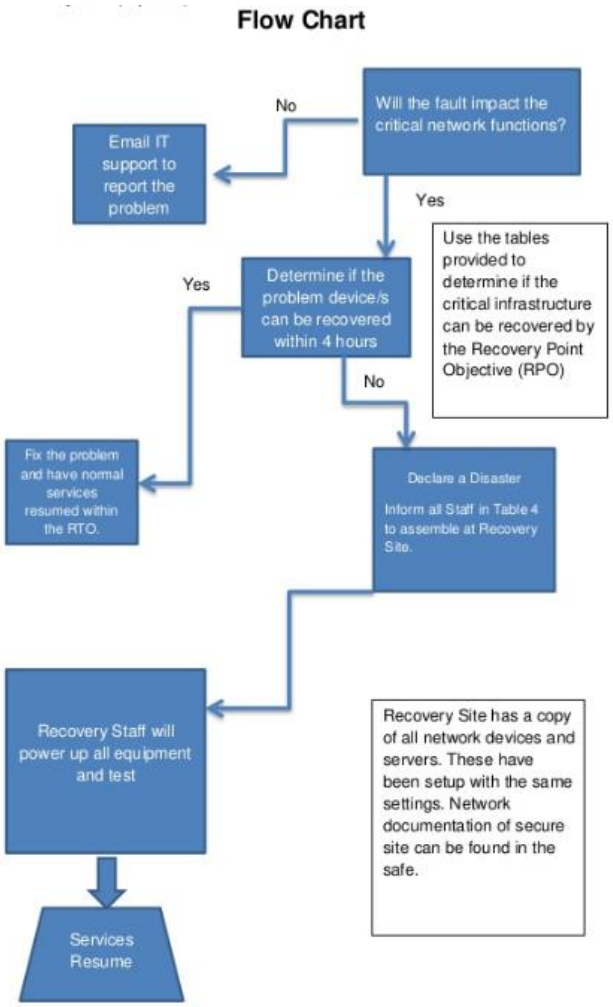
    a. The team must be able to effectively detect deviations in normal business operations in information systems and define if they represent an actual security incident.
    b. If incident declared, additional evidence collected and classification of the severity must be applied.
    c. Document of the “Who, What, Where, Why, and How”.
3. Containment:
    a. The immediate goal is to contain the incident and prevent it from inflicting further damage to the organization.
    b. Short term containment means to isolate affected systems and take down affected servers until incident resolved.
    c. Long term containment can involve applying temporary fixes to affected systems and rebuilding clean systems to bring back to recovery stage.
4. Eradication:
    a. Team must examine evidence and identify the root cause or location of the attack, remove the threat, and prevent similar attacks from happening in the future.
5. Recovery:
    a. Team will bring affected systems back online in a staged process to ensure another incident doesn’t take place. Extensive monitoring will be a crucial part of this stage.
6. Lessons Learnt:
    a. This stage should occur within two weeks of the incident that occurred, to ensure information and evidence remains fresh and relevant.
    b. The purpose of this phase is to complete documentation that could not occur during the live incident and also to investigate the response process and ascertain if anything could be done better or more efficiently.




The Vanderlay Industries information security program also has stringent disaster recovery planning, helping the organization prepare for unthinkable, and very unpredictable, situations that can greatly affect business operations. The disaster plan will implement controls to mitigate the impact the impact of a disaster and recover normal operations as quickly as possible.

The primary objectives of a disaster recovery plan is to develop, test, and document a well-structured and easily understood plan of action which will help the company recover as quickly and effectively as possible from an unforeseen scenario that interrupts information systems and business operations.

DRP Flowchart:




The planning for disaster recovery begins with a Business Impact Assessment (BIA). The BIA seeks to identify all of the potential threats facing the Vanderlay organization, assess and categorise the organisations vulnerability to those threats and then develop a list of risks that require intervention. With this list, the security team can plan to take action to mitigate to most significant of the identified risks and outline the facilities and technologies that would be needed to restore business operations as quickly as possible.

## The Role of SETA Programs at Vanderlay Industries.

The security education, training, and awareness (SETA) program of Vanderlay Industries has been developed to ensure that the information security program is effective in the medium and long term and that the security frameworks and day-to-day relevance remains in the forefronts of all staff members minds and activities.

SETA programs enhance security behaviour with all stakeholders by applying focus on correct information of security policy and industry best-practice. The primary benefits of the

Vanderlay Industries SETA program is that it will improve employee behaviour in a security context, will allow a process to be established to allow employees to report on potential security incidents, and that it will allow the organization to hold its staff accountable with matters regarding to security.

The Vanderlay Industries SETA program is primarily comprised of three key elements: security education; security training; and security awareness. Its overall purpose is to enhance and build a security centric mindset in three distinct ways: Building in-depth knowledge of operational security facets; developing skills and knowledge of underlying computer technology; and improving awareness for the need to be security conscious of all information assets in the organization.

To establish and implement the SETA program, Vanderlay Industries will outsource this operation to a third-party vendor who specializes in SETA and slowly integrate the work stream back in-house after a review in 12 months time. This review will assess the effectiveness of the SETA program and advise if the vendor needs to be retained or in-house sourcing can occur.

## Appendix:

- *Comprehensive list of all developed information security policies that fall under the Vanderlay Industries information security framework*:

Password Construction Guidelines

1. Statement of Guidelines

The passwords must be long and strong; the passwords should contain a minimum of 14 characters. It is recommended that passwords shall made up of multiple words. All work account in the organization should have a unique, different password. The password manager software that is offered by the organization shall be used in order to enable users to maintain multiple passwords. Also, enabling the use of multifactor authentication is recommended to ensure authentication

Long and strong passwords have the following characteristics:

• Contain 14 characters or more.

• Made up of multiple words

• Does not Contain personal information such as names, phone numbers, address, birthdates, and pets

• Does not Contain number patterns such as 1234, ABCD, or abcd1234

Password Protection Policy

1. Password Protection

1.1 Passwords shall have treated as a sensitive and confidential information; they must not be shared with anyone, nor inserted into any forms of electronic communication like email as a way of saving the password.

1.2 High-level employees like supervisors has no rights to get know the passwords of the low-level employees.

1.3 All passwords must be stored in the password manager's software that is provided by the organization

1.4 The feature of Remember Password on applications like web browser must not be used as a way of storing the password

2. Password Change

2.1 In case any password of the employees has compromised, the incident must be reported immediately to the IT team and the all passwords shall be changed

2.2 The InfoSec Team shall perform a password cracking operations periodically; and in case of cracked password, all password in the company shall be change to be in compliance with the Password Construction Guidelines

3. Password Creation

3.1 All passwords of the company users shall conform to the Password Construction Guidelines.

3.2 All passwords of the company users shall use a different and unique password for work accounts.

3.3 Users are not allowed to use any of their work related passwords accounts for their personal use

3.4 Accounts with system-level privileges shall have a unique password from all other accounts to access system-level privileges.

3.5 all privileged accounts shall use a multi-factor authentication

Risk Assessment Policy

1. The InfoSec Risk Assessment Team are responsible for executing the remediation programs on the company and developing it. All employees shall join the InfoSec Risk Assessment Team in the development of a remediation plan.

Disaster Recovery Plan Policy

1. Contingency Plans

• Succession Plan: in case the staff are not available to perform their duties, who is qualified to be in charge and takes full responsibility

• Data Study: categorizing all data stored in the system (the critical, and the confidential

• Computer Emergency Response Plan: What immediate actions shall be taken in consideration in the occurrence of such events, how to deal with it, who is to be contacted first and when

• Criticality of Service List: all the provided services by the organization must be listed based on their importance and their usage

• Data Backup and Restoration Plan: the backed up data must be detailed, as well as the media to which it is saved, and the place of the media. the times of completed backup shall be detailed and how the data could be recovered. the order of recovery in both long and short-term timeframes shall be detailed.

• Mass Media Management: Who is responsible of giving information to the mass, and in what occasions

• Equipment Replacement Plan: categories and list the important equipment for the company, what equipment is required for the company. Where this equipment from, and who is responsible for purchasing them.

Server Audit Policy

Policy

The company allows (internal and external Audit) to get access to its servers in which it allows the (audit organization) to perform ad hoc audits of all servers at the company.

1. Guidelines

In case of deploying server systems, a standard configuration template shall be used to

include:

• The central log review system must store all system logs

• The central patch deployment system must be used

• All actions of Administrator /Sudo must be logged

• The administrative group membership must be verified

• There shall be a periodically update and scan for the network in order to check the network shares and the network port that are in use.

• Antivirus programs shall be installed as a host security agent

• In case of making a significant change on the system or deploying it, a baselines shall be conducted

• The change control Board shall approve any changes might be conducted to the configuration template

2. Responsibility

All servers provided by the Company shall go through an audit process that are conducted by the Internal or External Audit Name

3. Specific Concerns

As some servers that is in use by the company stores a sensitive information of the company, inefficient configuration of such servers could lead to a loss of a secret information.

4. Relevant Findings

The tracking system shall contain all the relevant findings of the audit in order to get appropriate mitigating controls.

5. Ownership of Audit Report.

The company has a full right to obtain the findings generated by the <Internal or External Audit Name> within a week of project completion. All the findings shall be listed in a report form and owned by the company

Acceptable Encryption Policy

1. Algorithm Requirements

1.1 The set defined as AES-compatible according to the IETF/IRTF Cipher Catalog must conform with ciphers in use

1.2 NIST publication FIPS 140-2 defined standard for use must conform the algorithms in use according to date of implementation.

1.3 For the use of asymmetric encryption, the Elliptic Curve Cryptography (ECC) and RSA algorithms shall be used

2. Key Agreement and Authentication

2.1 Cryptographic protocols like IKE, and DiffieHellman must conform with the Key exchanges that is in use.

2.2 Before the derivation of session keys, the End points shall be authenticated

2.3 The authentication of the public keys shall be occurred prior to use in order to establish trust.

2.3 All servers like TACACS shall have a valid certificate signed by a known trusted provider.

3. Key Generation

3.1 The generation process of Cryptographic keys shall be held with full standards of security and safety manners in order to avoid any kind of loss, or compromise

3.2 The random number generator (RNG) industry shall be the standard of the generated key.

Communications Equipment Policy

1. It is necessary to install security tools like firewall and anti-virus into the communication equipment before they placed into service. Monitoring and administrator are the two roles for managing the communication equipment. The administrator role is to change the configuration parameters, where the monitoring role is to read configuration parameters only.

1.1 All issued commands by users will be recorded

1.2 With the usage of a secure protocol, all users shall authenticate through the central repository of users

1.3 Local users are not allowed to use communication equipment.

1.4 The Transmitted information from the device shall be encrypted

1.5 There should be a storage media that records all the events by the communication equipment.

1.6 This storage media must subject to a regular backup process

1.7 The password of the administrator user that manages the communication equipment should not be known by anyone in the organization.

Security Response Plan Policy

The InfoSec team are responsible for the Security Response Plan (SRP). They are responsible for developing, implementing, and the maintenance of a Security Response Plan.

1. Service or Product Description

The service that are to be deployed shall be defined by the product description in an SRP.

2. Contact Information

The SRP document shall contain the related information to all dedicated team members such as email addresses and phone numbers to be available during non-business hours in the cases of incidents or escalation. they might be called any time, and should be prepared for such situations.

3. Triage

The triage steps should be defined by the SRP in order to mitigate the security vulnerabilities with the help of security incident management team.

4. Identified Mitigations and Testing

The SRP shall contain remediation process that identifies mitigations and testing it before the process of deployment

5. Mitigation and Remediation Timelines

The SRP must define the expected timelines for repair based on impact to consumer, and company after the vulnerabilities has been identified by having a response guideline that shows the level of severity determined for the reported vulnerability.

Technology Equipment Disposal Policy

1. Technology Equipment Disposal

1.1 The technology assets must be sent to the disposal office once it’s no longer useful to use and all storage mediums shall be securely erased

1.2 The disk sanitizing software shall be used in order to remove all data including the licensed software, meeting Department of Defense standards

1.3 The technology equipment must not be sold to anyone

1.4 The computer equipment should be disposed in the electronic recycling bins that's locates around the company, not disposed landfill, or dumps.

1.5 The Equipment Disposal Team must remove all data prior to final disposal.

1.6 Utilizing the disk cleaning program in order to get rid of the electronic drives

1.7 There should be a sticker indicating that the disk has been wiped by the Equipment Disposal Team in the equipment case

1.8 The sticker should include the name and the ID number of the technician who performed the disk wipe

2. Employee Purchase of Disposed Equipment

2.1 The employee of the company would be able to purchase the equipment that are no longer needed in the company or has reached the end of its useful life

2.2 The lottery process will be used in the equipment purchases

2.3 The cost of the equipment and the item will be determined by the finance and information technology.

2.4 Employees cannot purchase their office computer

2.5 The sold equipment won't contain any warranty

2.6 Not working equipment will be disposal or donated.

## References:


1. Whitman, Michael E. Mattford, Herbert J. 2017. Management of Information Security. *Information Security*, 5th Edition. Published via Cengage Learning. Boston MA. USA.
2. Giles, Timothy D. 2009. How to Develop and Implement a Security Master Plan. Published via CRC Press. Boca Raton, FL. USA.
3. NIST SP 800-18, Rev. 1: Guide for Developing Security Plans for Federal Information Systems.
4. NIST SP 800-12: An Introduction to Computer Security: The NIST Handbook
5. NIST SP 800-14: Generally Accepted Principles and Practices for Securing Information Security Systems.
6. NIST SP 800-100: Information Security Handbook: A Guide for Managers.
7. Koutsakis, Polychronis. 2021. Lecture Recordings (2-10). *ICT380 Information Security Policy and Governance*. Murdoch University. Perth, WA. Australia.
8. SANS Institute. 2021. Security Policy Templates. Accessed via "Information Security Policy Templates | SANS Institute". SANS Institute.
9. PurpleSec. 2021. Comprehensive IT Policy. Published via PurpleSec LLC. USA.

10. Falcon, Jeff. 2020. The Importance of Incident Response and Disaster Recovery Planning. Published via the 'Solutions Blog- Insights From Experts Who Get IT'. [The Importance of Incident Response and Disaster Recovery Planning | CDW Solutions Blog]
11. Various Authors, 2021. CaTS Information Technology- Policies. 'Wright State University' Accessed via: [Policies | CaTS | Information Technology | Wright State University]. Wright State University. Dayton, Ohio. USA.
12. Weinberg, Neal. 2021. Business Continuity and disaster recovery planning: The basics. 'CSO Australia'. Accessed via [Business continuity and disaster recovery planning: The basics | CSO Online]