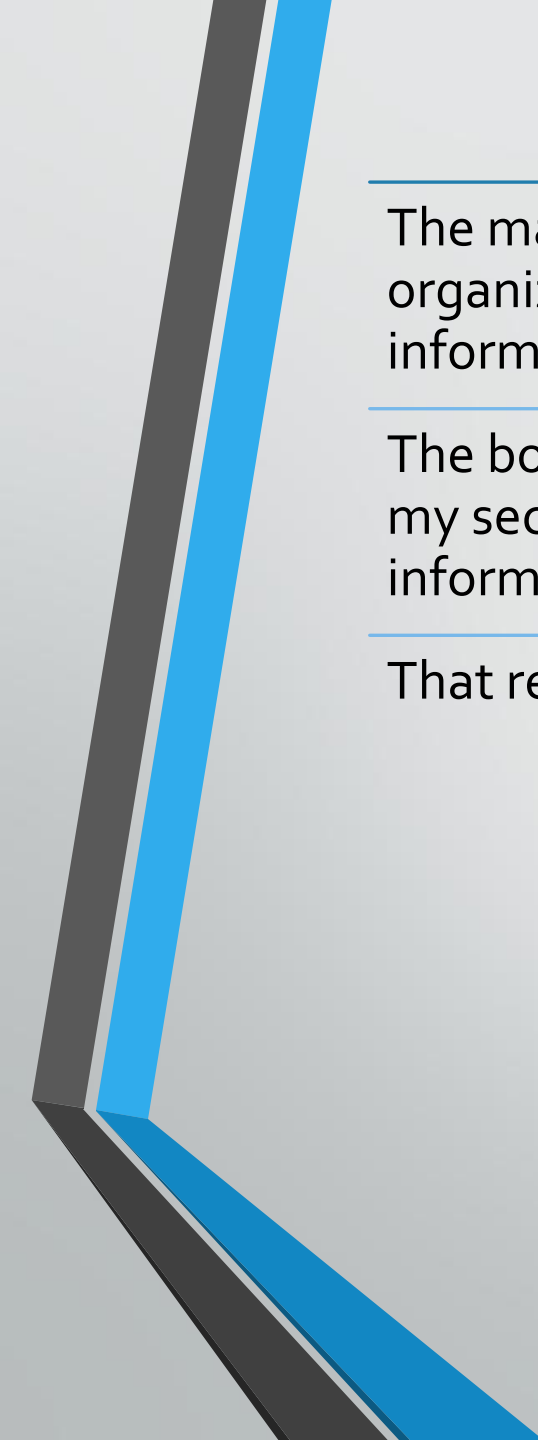




Security Program Implementation Plan

By: Ramon Lopez



The manager has asked me to write a security implementation plan for the organization's new data center. This data center will store sensitive customer information that is critical to the customers and to the organization.

The board of directors have decided a reasonable budget will be put in place to make my security implementation plan work and to protect the customer's sensitive information.

That reasonable budget will be **\$250,000**.

Context

What Will Be Needed?



- To have a successful security implementation plan, the following areas will be covered:
 - The legal and ethical side of the information.
 - Planning for the security aspect.
 - The risk management aspect.
 - The use of security tools.
 - The use of physical security.



The Legal & Ethical Issues of The Information



Why Should We Care?

It is obvious that we do not want to break any laws that is in the western region and get fined for it.

The laws we want to look into are:

The civil ones

The criminal ones

Regulatory and/or Administrative ones

Privacy

- There are things that we should consider, these things are:
 - Privacy
 - Keeping people's information safe from unauthorized access.
 - U.S. Regulations:
 - Privacy of Customer Information Section of the Common Carrier Regulation:
 - "A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts," (Legal Information Institute, n.d., Paragraph 2).

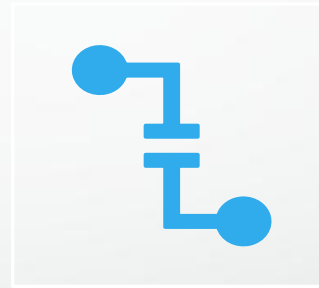
Following Payment Card Industry Data Security Standards



Why do this?

To protect customer's card information from unauthorized users.

It is designed to enhanced security to the customer's account data.



It addressed in five areas:

Build and maintain a secure network.

Have a vulnerability management program.

Have strong access control measures.

Frequently test and monitor networks.

Have an information security policy.


Ethics




- We will want to follow the Ten Commandments of Computer Ethics.
- Use a code of ethics that has been established by many professional organizations.
- We will want to train the employees to be aware of:
 - The expected behavior of an ethical employee.
 - Also, to train in many different security aspects.
- This is needed to have a well-prepped system user.
- If failed, we will use the three conditions needed to deter unethical behavior.

Understanding The Regulations


Our information security professionals will need to look into the regulations of the region. This is because federal regulations will not apply to our organization.



This is to ensure that our organization is in compliance with the region's regulations.



Planning for The Security Aspect



Using a Policy



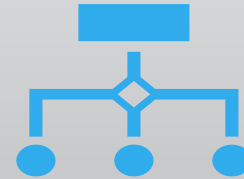
- Using a policy will establish what is and is not acceptable behavior.
- Have employees properly read the policy so that it is understood and followed.
- Have the policy be managed by every change.
- Needs to have:
 - A manager
 - Scheduled reviews
 - Making recommendations for reviews
 - A revision date

Using Issue-Specific Security Policy



This will allow us to:

- State our policy
- Which equipment is authorized to be used.
- Prohibit which equipment cannot be used.
- State the consequences of a violation of the policy.
- Our policy review and modification, if needed.
- And limit our limitations of liability.



This will be used to set our standards to our employees who will be working at the data center.

Using an Information Security Blueprint



- Using an information security blueprint will allow us to:
 - Design
 - Select
 - Implement
- An information security blueprint will be the basis for our security policy.
- We will use the ISO 27000 Series, this:
 - Will provide management direction and support.
 - Give recommendations for information security management.
 - Will serve as a starting point.

Implementing a S.E.T.A. Program

Use of a training security program will:

- Educate
- Train
- Aware

This program will require everybody to go through this program to avoid accidental security breaches.

It will enhance skills needed to avoid these types of accidents.

The Use of Plans

- Using plans will allow us have an idea what to do when something happens.
- We will need to incorporate:
 - An incident response plan
 - A disaster recovery plan
 - And a business continuity plan
- Also, will need a Business Impact Analysis, this will be need to assets the effect of an attack to our organization.



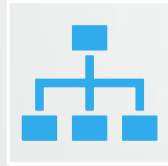
Managing The Risks

Identifying The Risks



Have our Information Security Professionals to:

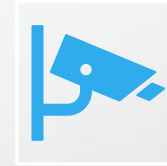
Identify
Classify
Prioritize



This will ensure that our organization has people to protect our organization's information assets.



Have each asset be conducted with a threat assessment.



This will ensure that we know what threat each asset faces.

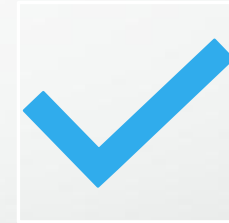
Planning The Process



Create a project management principle to begin the risk identification process.



Organize a team of people who will be representing all affected groups within the organization.



The following items must be discussed:

- Reviews
- Tasks
- Assignments
- Timetables

Asset Identification



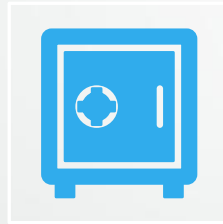
Identify all our assets in the building:

Equipment

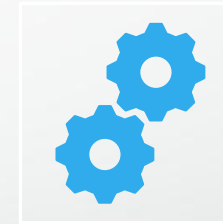
People

Data Information

Software

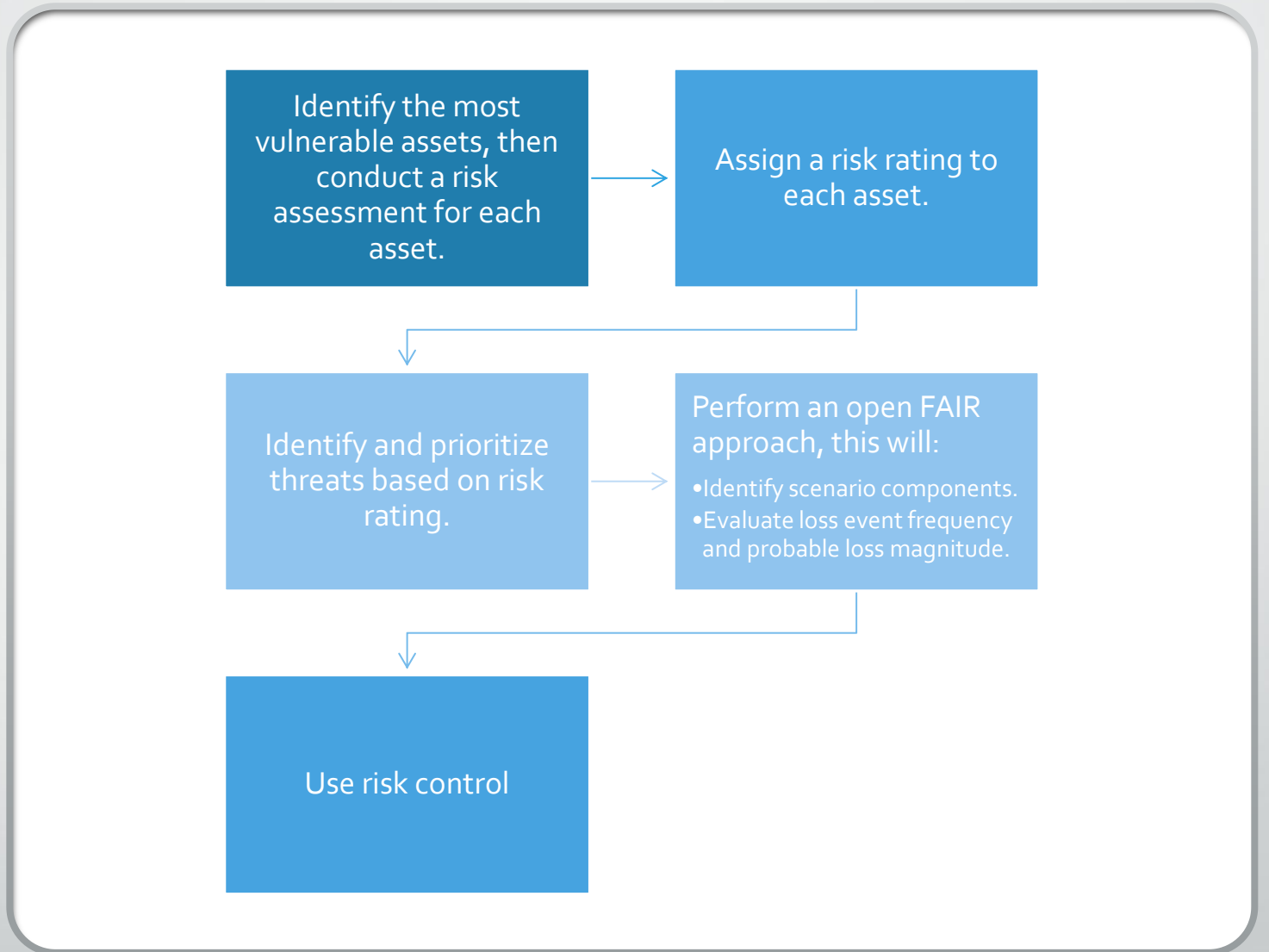


This will help the organization be effective at protecting the assets.



To make this process faster, use an automated tool that can identify our system's elements.

Risk Assessment



Risk Control (1/2)

- Complete a ranked vulnerability risk sheet, once this is completed, pick at least one:
 - Defense:
 - The attempt to prevent exploitation.
 - Transference:
 - The attempt to shift risks to other assets.
 - If can not be handled, transfer the risk to another organization.
- Mitigation:
 - The attempt to reduce the impact of an attack.
- Acceptance:
 - The process of not protecting the assets.
 - Asset does not justify the cost of protecting it.
- Termination:
 - Avoid activates that could introduce uncontrollable risks.



Risk Control (2/2)

- Select a risk control strategy based on:
 - Is there a vulnerability?
 - The vulnerability can be exploited.
 - The potential loss is substantial.
- Implement, monitor, and assets risk control.
- Document the results of the risk control.
- For a comprehensive process, use the NIST Risk Management Framework.



Using Security Tools

Access Controls

- Have systems select who may use the device and how they use it.
- Include these four mechanisms:
 - Identification:
 - Requires a validation of a user's identity.
 - Authentication:
 - Have users enter either a password or passphrase.
 - Or use either a dumb card or smart card.
 - Authorization:
 - Requires users to enter a matching authentication to grant access.
 - Accountability:
 - Have the system record who used which device at which time to keep track of uses.

The Use of Biometrics

Use it to measure human traits to authenticate identity.

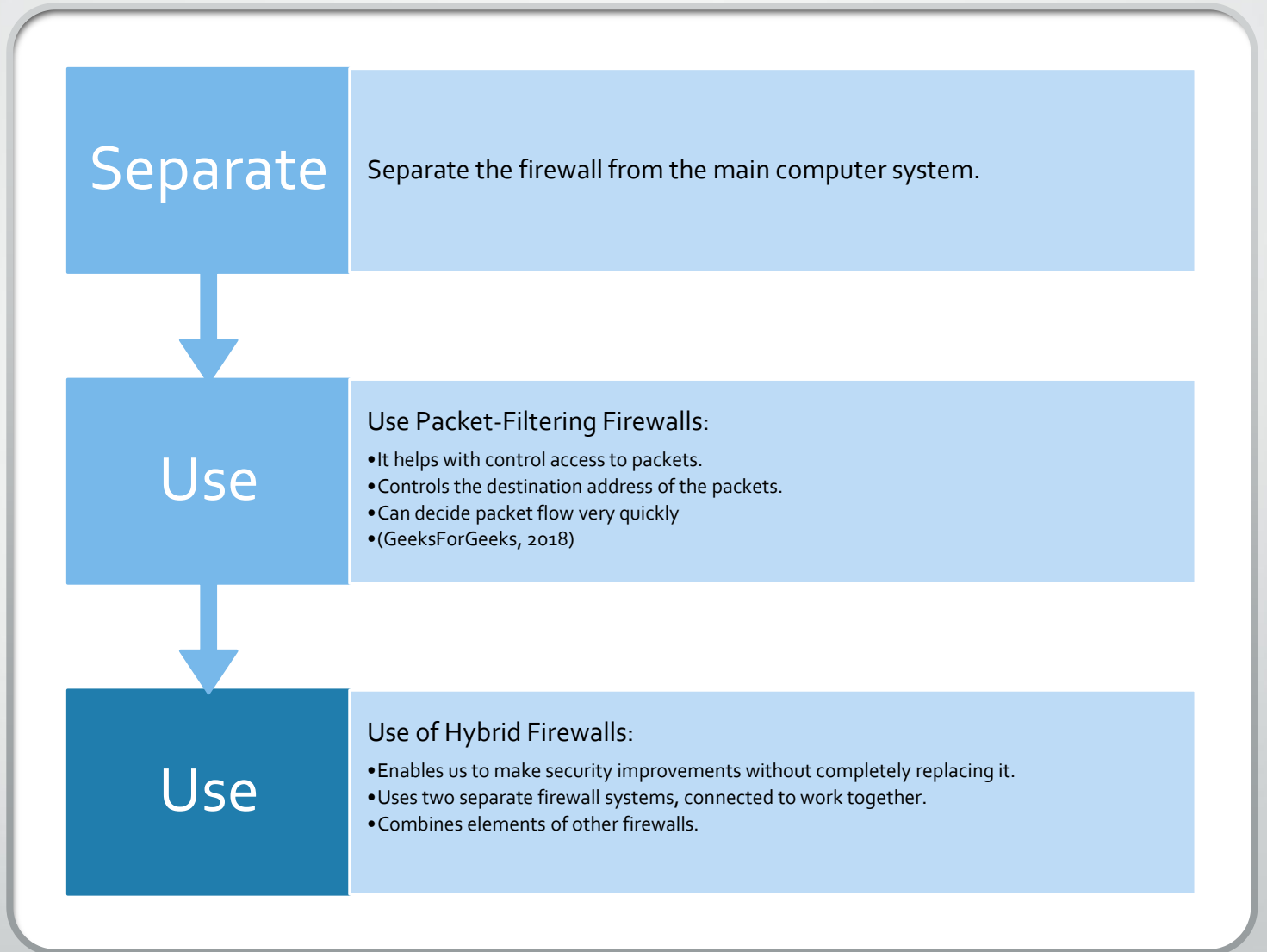
To make it unique:

- Use fingerprints
- The retina of the eye
- The iris of the eye

Evaluate:

- False reject rate
- False accept rate
- Crossover rate

Using Firewalls



Configuring The Firewall

Set each firewall device with its own set of configuration rules.

This will regulate actions within the organization.

Setting firewall rules:

- Examine data packets
- Perform comparison with predetermine logical rules.
- Set anti-spoofing filters.
- User permit rules.
- Management permit rules.
- (Richards, 2018).

Use a software appliance to allow administrators to restrict content.



Using Physical Security



Access and Security Controls

- Have the facility be surrounded with protection mechanisms.
- Protection Measures Include:
 - The use of walls, fences, or gates.
 - Hire guards to protect the facility.
 - Acquire guard dogs to assist the guards.
 - Have all members of the facility display ID cards.
 - Lock the most important rooms using mechanical locks.
 - Use mantraps around those important rooms.
 - Use electronic monitoring.
 - Have an alarm system put in place.

Fire Detection and Response

- Protect important rooms with:
 - A fire suppression system that is used to detect and respond to fires.
 - Denying a room of temperature, fuel, or oxygen, use:
 - Water mist system
 - Soda acid system
 - Gas-based system
- An automatic fire detection system.
- A fire suppression system that:
 - Are both automatic and manual.
 - Use both:
 - Class A: For ordinary combustible materials.
 - Class C: Energized electrical equipment.
 - (Brain O'Connor, 2021)

Other Things to Consider



Supporting utilities, these can include:

Heating
Ventilation
Air Conditioning
Water
Power



Stay within the load limits of the building to avoid structural collapse.



Consistently document, evaluate, and test facilities capabilities.



References

- GeeksForGeeks. (2018, November 2). *Types of firewall and possible attacks* - *GeeksforGeeks*. GeeksforGeeks. <https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/>
- Legal Information Institute. (n.d.). *47 U.S. Code § 222 - Privacy of customer information*. LII / Legal Information Institute. <https://www.law.cornell.edu/uscode/text/47/222>
- O'Connor, B. (2021, July 16). *Fire Extinguisher Types* | NFPA. Wwww.nfpa.org. <https://www.nfpa.org/News-and-Research/Publications-and-media/Blogs-Landing-Page/NFPA-Today/Blog-Posts/2021/07/16/Fire-Extinguisher-Types#:~:text=Fire%20Extinguisher%20Types%20%20%20Class%20of%20Fire>
- Richards, D. (2018, May 1). *Best Practices for Firewall Rules*. Liquid Web. <https://www.liquidweb.com/kb/best-practices-for-firewall-rules/#:~:text=SANS%20Institute%E2%80%99s%20Firewall%20Checklist%2C%20under%20Security%20Elements%2C%20recommends>
- Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6th ed.). Cengage Learning.