Port of Seattle IT Security Risk Assessment

Joseph Sanchez

Central Washington University

December 4, 2018

Table of Contents

Executive Summary

Overview of Assessment

When the assessment took place, I interviewed Oscar Segura who works for Port of Seattle. During our interview, the information asset we assessed was employee account information. The assessment took place on November 7, 2018. The purpose of assessing employees' account information was to see what are the chances that the employee's account information would be compromised.

Identified Risks and Common Risk Themes

There were some area of concerns that I have discovered while the assessment was in-progress. One of those concerns was a disgruntled employee may release an employee's account information. Other areas that were also a concern was a hacker may gain access to employee's account information in the following ways. An intruder could gain access to the access panel on the parking garage fare kiosk and plug a hacking device such as a keyboard or a flash drive. The Wi-Fi connection from the internal network to the parking garage fare kiosk machine could be intercepted by an unauthorized individual. Finally, an unauthorized individual could access the room where the locked containers are stored.

These are the different risk areas that I found within my assessment at the Port of Seattle.

Summary of Proposed Mitigation Activities

The common thing to do when you are mitigating risks is to first start with the basic assessment. A basic assessment can be something like evaluating the systems settings that has been set by default; such as a type of encryption, is the computer's hard drive encryption enabled or disabled, internet security settings configured or not, etc. these are the general things that would need to be examined before deciding which security controls to implement to the computer system.

The proposed mitigation methods are dependent on the area of concerns and findings that were found during the assessment. For example, an intruder using Wi-Fi to try to obtain information from the kiosk machine is an area of concern. So, this is the area that will be assessed and findings that were found would be the evidence to determine which security control would be appropriate to implement that will resolve this area of concern. Generally, you would first figure out what basic security controls are in place and possible vulnerabilities that may occur when evaluating computer system and its infrastructure.

Risk Assessment Report

Overview of Risk Assessment

I used Octave Allegro methodology method to help me get a better understanding on what areas to assess and see what the potential impact on those areas would be. For example, Oscar has provided me the information such as the percentages for worksheet 1 through 3 on the different levels of each impact area. The usage of the Octave Allegro worksheets has provided me a better insight as to what kind of questions I could ask Oscar.

During the interview, I have taken Oscar's comments and wrote them down in the appropriate box where it best suited. How we approach different stages of the Allegro worksheets was, both of us worked on them in chronological order. On worksheets 1 through 5, we give each of the impact areas a number value that best fit for different risk values. I also asked him how the Port of Seattle would rank their priority on the different impact areas mentioned on worksheet 7. Oscar gave me a series of numbers from 1 through 5 and assigned a number value from the most important to the least important in Port of Seattle's point of view.

This is how I followed the methodology. I used it as a guide and took what the methodology was asking. I tailored my answers that I received from the interview and then applied them to the worksheets. Other methods I used was the example risk assessment report from Introducing Allegro document, so I can get an idea of what the report should look like and see what kind of information was in each of the boxes.

I completed the rest of the worksheets that were part of the risk assessment. For example, on worksheet 8 where it said critical asset, I chose to put employee account information under that specific box; then I provided a description and a reason why that asset is important to Port of Seattle. All three sections of worksheet 9, the container description states the type of container and the type of information in the container.

Port of Seattle has made the decision that employee account information is consider an information asset because it has sensitive information about the staff members which has value to organization. The type of containers that Port of Seattle decided to use to store employee records is a server, databases, and workstations. Employees can access the information to perform necessary duties as well as archive the information.

The Port of Seattle must use the servers, databases and workstations to perform their operation which revealed some area of concerns. If a disgruntled employee accesses and releases employee's information is one concern. Another if a hacker was to gain access and steal employees' information, and other concerns were found. These are the areas the Port of Seattle wanted assessed to see what vulnerabilities exist, what security measures are in place, and test the security of those systems.

Risk Measurement Criteria

The following impact areas are what Oscar and I determined needed to be assessed. They are *reputation and customer confidence, financial, productivity, safety and health, and fines and legal penalties.* In each of these areas, Oscar and I have agreed that safety and health will be ranked number 5 meaning that this area is the most important. Followed by fines and legal penalties which was ranked number 4, the second most important. Other impact areas were

prioritized according: reputation and customer confidence was ranked number 3. Financial was ranked number 2, and productivity number 1.

The threshold for each of different impact areas were rated according to the following. Low was measured as 1% or less. Medium was measured from 2% to 9%. High was measured as 10% or higher.

Scope of Assessment

Oscar and I identified employee account information as an information asset. The employee account information contains personal information about the employee(s). The account data includes social security numbers, bank account and routing numbers, earning statements, credit card information, etc. Since this information asset contains a lot of sensitive data, the Port of Seattle wanted to assess the vulnerabilities to unauthorized access to the account information and the impact to its operation.

Security Controls Assessed

Table 1. Security Control Assessment

Critical Security Control Identifier	Assessment of Security Control	Results of Assessment
CSC 1.1	Interviewed Oscar Segura (Information Security Engineer)	CSC 1.1 control has been implemented
CSC 1.2	Interviewed Oscar Segura (Information Security Engineer)	CSC 1.2 control have been implemented.
CSC 1.3	Interviewed Oscar Segura (Information Security Engineer)	CSC 1.3 control have been implemented.
CSC 1.4	Interviewed Oscar Segura (Information Security Engineer)	CSC 1.4 control have been implemented.
CSC 1.5	Interviewed Oscar Segura (Information Security Engineer)	CSC 1.5 control has not yet been implemented
CSC 1.6	Interviewed Oscar Segura (Information Security Engineer)	CSC 1.6 control has been implemented.
CSC 2.1	Interviewed Oscar Segura (Information Security Engineer)	CSC 2.1 control has been implemented
CSC 2.2	Interviewed Oscar Segura (Information Security Engineer)	CSC 2.2 control has been implemented
CSC 2.3	Interviewed Oscar Segura (Information Security Engineer)	. CSC 2.3 control has been implemented
CSC 2.4	Interviewed Oscar Segura (Information Security Engineer)	CSC 2.4 control has been implemented
CSC 3.1	Interviewed Oscar Segura (Information Security Engineer)	CSC control 3.1 has not been implemented yet.

CSC 3.2	Interviewed Oscar Segura (Information Security Engineer)	CSC control 3.2 has been implemented
CSC 3.3	Interviewed Oscar Segura (Information Security Engineer)	CSC control 3.3 has been implemented.
CSC 3.4	Interviewed Oscar Segura (Information Security Engineer)	CSC control 3.4 isn't fully implemented.
CSC 3.5	Interviewed Oscar Segura (Information Security Engineer)	CSC control 3.5 has been implemented.
CSC 3.6	Interviewed Oscar Segura (Information Security Engineer)	CSC control 3.6 has not been implemented.
CSC 3.7	Interviewed Oscar Segura (Information Security Engineer)	CSC control 3.7 has been implemented
CSC 4.1	Interviewed Oscar Segura (Information Security Engineer)	CSC Control 4.1 has been implemented.
CSC 4.2	Interviewed Oscar Segura (Information Security Engineer)	CSC Control 4.2 has been implemented.
CSC 4.3	Interviewed Oscar Segura (Information Security Engineer)	CSC control 4.3 has been implemented.
CSC 4.4	Interviewed Oscar Segura (Information Security Engineer)	CSC Control 4.4 has been implemented.
CSC 4.5	Interviewed Oscar Segura (Information Security Engineer)	CSC control 4.5 has been implemented.
CSC 4.6	Interviewed Oscar Segura (Information Security Engineer)	CSC control 4.6 has been implemented.
CSC 4.7	Interviewed Oscar Segura (Information Security Engineer)	CSC Control 4.7 has been implemented.
CSC 4.8	Interviewed Oscar Segura (Information Security Engineer)	CSC control 4.8 has not been implemented.
CSC 5.1	Interviewed Oscar Segura (Information Security Engineer)	CSC control 5.1 has been implemented.
CSC 5.2	Interviewed Oscar Segura (Information Security Engineer)	CSC control 5.2 has been implemented.
CSC 5.3	Interviewed Oscar Segura (Information Security Engineer)	CSC control 5.3 has been implemented.
CSC 5.4	Interviewed Oscar Segura (Information Security Engineer)	CSC control 5.4 has been implemented.
CSC 5.5	Interviewed Oscar Segura (Information Security Engineer)	CSC control 5.5 is implemented.
CSC 5.6	Interviewed Oscar Segura (Information Security Engineer)	CSC Control 5.6 has not fully been implemented.
CSC 5.7	Interviewed Oscar Segura (Information Security Engineer)	CSC control 5.7 has been implemented.
CSC 5.8	Interviewed Oscar Segura (Information Security Engineer)	CSC control 5.8 has been implemented.
CSC 5.9	Interviewed Oscar Segura (Information Security Engineer)	CSC control 5.9 has been implemented.

Areas of Concern (or Risks)

Disgruntled employee may access and release employee's account information

- Threat statement: A disgruntled employee may release an employee's account information.

  Finding: A disgruntled employee could use their access badge to gain access to the system, steal data and release it to the public. If the configurations of a firewall and malware defense software was configured improperly, an employee could compromise administrative accounts, exploit servers, etc. which could lead to an alteration of employee's information or possibly be leaked.

- Evidence: The evidence that I have gathered is that all employees have access badges and passwords to gain access to the building and Port of Seattle's computer network(s), along with their servers and workstations. CSC control 3.1 has not yet been implemented across Port of Seattle's computers systems. The secure configurations of operating systems and software has not yet been a standard procedure for Port of Seattle, but they are in the process of incorporating it across their computer systems.

- CSC control 3.5 would be compromised if the breach was to occur. The file integrity check tools may not be able to function properly and catch unauthorized changes to the files within the system.

- Impact: Employees may be very concern if their account information was released to the public or used by criminal entities. The level of confidence the employees have with Port of Seattle would be severely impacted. Which could harm Port of Seattle's reputation. The impact area reputation and customer confidence were valued at high.

- If an employee's financial data was released or altered it could prevent the employee from being paid and their funds vulnerable to theft. The chances of employee's financial information becoming compromised less likely, but the damage could be significant, which is why the risk level is valued at medium.

Hacker gain access to employee's account information

- Threat statement: A hacker may gain access to employee's account information.
- Finding: One of the ways that the hacker could gain access to employee records is finding a vulnerability in one of the security controls and exploiting it to bypass the other security controls. Or the security authentication services may not have been properly configured.

Other possible areas that could be exploited is the maintenance of the system may not be up to date.

- Evidence: CSC control 3.4 has not been implemented completely. Port of Seattle is still assessing on how to address Remote Desktop Protocol (RDP) since it is not actively support a strong encryption. Their solution is to use a multi-factor authentication protocol (2FA) to strengthen RDP's encryption during remote sessions.

- CSC control 1.5 has not been applied yet. But Port of Seattle is currently in the process of incorporating 802.1x authentication protocol to their networks, to help reduce the number of devices being able to connect to their network. So, they don't have to rely on a VPN service for adding a limitation of how many devices can connect to their network infrastructure.

- Impact: An impact on reputation and customer confidence category, the risk level is medium. The reason why the risk value is medium because the Port of Seattle would do an extensive risk assessment and find out the damage done and how their reputation was affected. It may require them to re-establish trust with their staff members. It is not a total loss; but a setback.

- If a hacker was able to retrieve financial records such as Port of Seattle's account and routing numbers, it could cause them to lose a lot of money. It also could setback their productivity, which would affect their ability to get things done (projects, upgrades, etc.). The impact value for financial area is a medium as well; because the organization can still operate even if the hacker syphon funds from their account. They would still need to retrieve their funds from either other government agencies or their own reserves.

An intruder could gain access to an access panel at the kiosk machine

- Threat statement: An intruder could gain access to an access panel to plug in their hacking device (like a keyboard or flash drive) into a kiosk machine at a parking lot.

- Finding: The access panel on the kiosk machine is visible to the public. Since the access panel to the kiosk machine is expose, an intruder could break into the access panel and see what access points are visible to exploit the Kiosk computer. One of the features on the kiosk computer are USB ports.
- Since there are USB ports, the intruder could plug in a keyboard or a flash drive to hack the kiosk's operating system or its configurations by inserting commands to download the data to a removeable media device.

- Evidence: Authorized personnel may have a key or another way to gain access to kiosk machine. One of the ways that the intruder could can gain access to that computer is by staying hidden somewhere while maintaining line of sight to see how the authorize

employee is able to get into that computer; then use that method or steal the key from the employee to break in.

- Security control 1.4 can be exploited. The security control 1.4 may think that an external device that was plugged into the kiosk is an authorized device but, it's an intruder device compromising the security control 1.4. Another security control that may not provide the necessary protection is security control 2.3. Even though a security control was implemented and scans every computer system and device across its network, an unknown device could get pass the software inventory tools.

- Security control 3.1 would not have provided the protection it needed for the kiosk machine because the system's configuration would have been compromised and no longer secure if the intruder was able to modify it.

- Impact: Based on the findings that I have received shows that the impact area of reputation and customer confidence is high. My reasoning as to why the impact value is high is because the kiosk machine in the parking lot contains information such as credit card information, name of the person, vehicle license plate number, etc. All this information is stored at the kiosk machine as an employee enters their information to pay for parking.

- If the kiosk booth was to get hacked, all the personal information stored would be in jeopardy of theft. If the breach occurred, the cost of reconfiguration, amount of labor hours, and re-securing the kiosk computer could be financially intensive. In this case, financial area could be impacted severely depending on the extent of the breach.

An intruder intercepting the Wi-Fi signal to obtain information

- Threat statement: An intruder intercepting the Wi-Fi signal between the kiosk computer and the network to steal personal information from the kiosk computer.

- Finding: An adversary could use the Wi-Fi signal to gain access and compromise the server or workstation that contains employee information from the kiosk. A workstation could be used as a server for the kiosk machines. If an adversary was able to establish a connection to workstation, they could use that workstation as an exploitation tool to reach the kiosk. Once they got a foothold on the server or network, they could exploit other vulnerabilities within that system to gain elevated credentials; and move laterally to obtain domain credentials and use it to continue to infiltrate the environment and establish a counter measure to prevent detection.

- Kiosk computers uses Wi-Fi to connect wireless access point to be able communicate with Port of Seattle's internal network. The Wi-Fi has security encryption implement to protect the data that is being transferred over a wireless network.

- Evidence: The kiosk booth is accessible to employees and non-Port of Seattle employees. Contractors and Port of Seattle staff members use the booth to purchase parking passes (day pass, weekly or monthly passes). The information is sent to Port of Seattle's centralized database.

- Security control 3.1 would not provide the necessary protection that the computer needs. The secure configuration of the operating system would be changed by the adversary when they changed the system's security settings. Another reason, Port of Seattle has not yet made secure configuration of operating system and software applications a default standard procedure.

- Security control 3.2 is providing the necessary protection for kiosks by using a strict configuration procedure. For example, when a new kiosk computer is being implemented IT department installs all the necessary hardware and software components in an isolated environment. This also applies to infected systems. They examine the level of encryption being used for the Wi-Fi network such as WPA-2 Enterprise encryption.

- Port of Seattle has not fully implemented CSC security control 4.2, but they still utilize some of the features under that security control. They use Security Information and Event Management (SIEM) tool and other vulnerability tools to analyze the system's behavior via event logs. They also analyze the Wi-Fi traffic and its behavior with network analyzer software such as Wireshark. Once the information has been gathered they can use the event logs to make a comparison.

- Impact: When an adversary has control of a server or database, they can cause further damage to that system such as deleting files off the server or database. A full system analysis may be conducted by Port of Seattle's IT Department to find out what specific files has been deleted and see how the breach happened. Other staff members in another department could raise questions to those security standards that have been applied. In this area of concern, reputation and customer confidence has been rated to be high. Encryption process for network and database could be exposed.

- Port of Seattle's corporate account funds could become depleted by unauthorize charges on the account. The cost of repairs and labor hours can be intensive, depending on severity of damage done to the database or servers and other computer systems. So, the level of impact on finance has been rated to be high.

- The productivity may be affected, which could affect some employee's ability to meet deadlines depending on what department they are assigned. But the entire Port of Seattle would not shut down.

A thief gaining access to the locked container

- Threat statement: A Thief locating and gaining access to the account information store in the locked containers.

- Finding: A thief may use social engineering to trick an employee into giving elevated access privileges, so they can access the confidential data. One of the ways that the thief can get that access is by impersonating one of the workers at Port of Seattle and get into the building with the necessary credentials. Another option could be using the identity of an approved computer to get pass the security controls that Port of Seattle have set.

- Evidence: All Port of Seattle employees have badges to get into the building and have different access privileges which allows them to enter different areas throughout the building. The thief could pick-pocket one of the employees and take their badge or use a handheld scanner to steal the data off the badge and make their own access badge. The thief would use the access badge to trick the key card security system to get into the archive room.
- CSC security control 4.1, was not used as frequently to test the security and validate the potential vulnerabilities of the key card security system. Also, testing was not done to determine the effectiveness of the key card security system.

- Impact: Staff members could get trouble by the organization for not securing the container properly; or the thief could exploit the organization by using the contents of information as leverage. The risk level is medium, because the chances of Port of Seattle will give into the thief's demands is less likely.

- The chances of Port of Seattle getting sued by one of their own employees is likely. But if an employee decides to sue the Port of Seattle for their identity being stolen, they may be required to pay restitution. The organization will make changes to infrastructure and security procedures.

Risk Heat Map

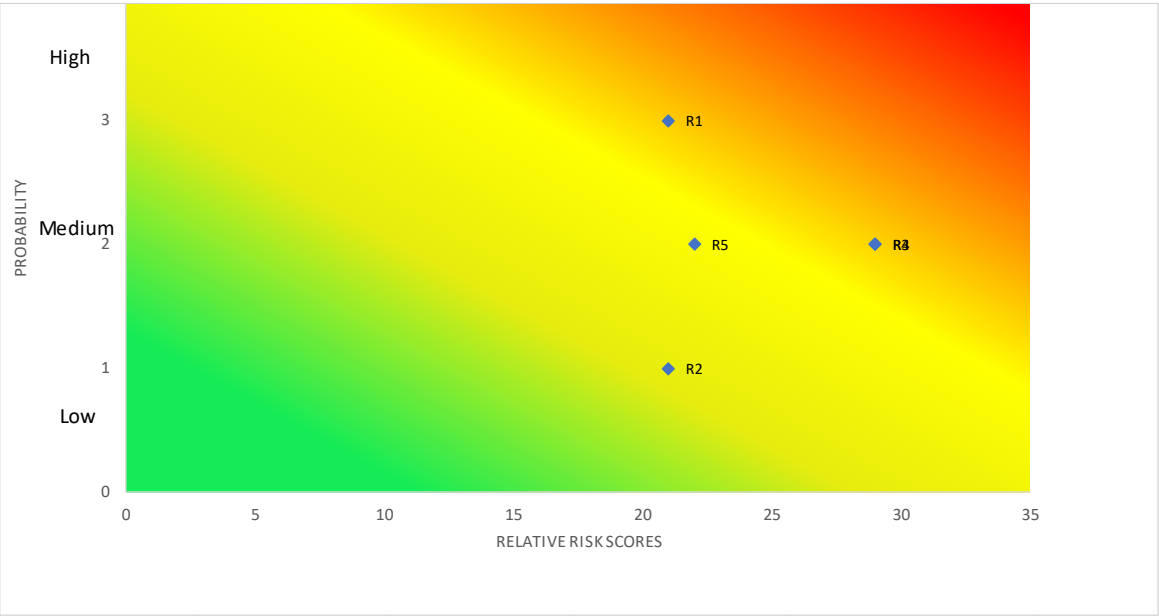

Table			Legend			
Area of Concern	Probability	Relative Risk Sco	Area of Concern	Probability	Relative Risk S	Level of Probabil
R1	3	21	R1 - disgruntled employee may release an employee's account information	High	21	**1 - Low**
R2	1	21	R2 -hacker may gain access to employee's account information.	Low	21	**2 - Medium**
R3	2	29	R3 - intruder could gain access to the access panel to plug in their hacking device (like keyboard or rubber ducky USB drive) at kiosk machine.	Medium	29	**3 - High**
R4	2	29	R4 - intruder being able to use WIFI to obtain information from the Kiosk machine	Medium	29	
R5	2	22	R5 - Thief trying to get access to a room where locked containers are stored.	Medium	22	

Risk Mitigation

Risks to Accept

N/A

Risks to Defer

N/A

Risks to Transfer

N/A

Risks to Mitigate

Risk Mitigated: disgruntled employee may release an employee's account information.

A disgruntled employee could release employee data, so the Port of Seattle decided to mitigate because it was likely this threat to occur. To minimize the threat, there are various methods which could help reduce the chance of the data being released by a disgruntled employee. The options are applying security controls 1.4, 3.4, and 3.5. Other ways that will help reduce the impact is strengthening the security controls to the database and enabling permission controls to the files.

By adding permission controls to files in the database, it prevents users from being able to access files for those who does not have proper permission. The approximate start date is February 2019 to Mid-March, 2019 for implementation of security controls and enabling permission controls to files in the database. You also want to add or enhance access controls and encryption tools to workstations including laptop and desktop computers. For laptop computers, you may want to encrypt the hard drive just in case the computer was lost or stolen, so the data can still be protected from prying eyes. The Port of Seattle's IT department will be responsible for the completion of this risk mitigation. A follow-up assessment will take place once quarter to check on the effectiveness of the security controls that have been implemented.

After mitigations efforts are in place, a comparison of the before and after results will be performed. If the after results of the risk is lower than before results, then the organization will consider the risk to be acceptable and further mitigation is not necessary.

Risk Mitigated: Hacker gain access to employee's account information

The reason mitigation is necessary for a dedicated archive database was the archive database has older information that is used by employees from time to time. Port of Seattle decide mitigation was necessary. The information that is stored on the database still needs to be protected from outside threats. Oscar has made the decision to elevate the security of the database to decrease the amount of vulnerabilities even further. Oscar has decided on the following solutions, they

would install a two-way authentication process, add USB-based login method with an encryption process embedded into the flash drive, virtual private network (VPN) software, and dedicated personnel to handle the arching of files.

Each of these options will provide the necessary protection to the archive database. Which minimizes the chance of a hacker or unauthorized person the ability to steal data and cause damage to the Port of Seattle's database. A start date for implementing of these security measures will be approximately June 2019 to December 2019. The Information security team and human resource department will be the one who will be responsible for the upgrades that will be made to database and other system infrastructure. The reason why human resources would be involved in this risk mitigation is because they are the ones who make the decision for approving upgrades and knows exactly how much money is in each account. HR oversees the entire project.

The information security team handles the specifics of the upgrades and implements them to improve security to the computer system(s). This can include things like what network authentication protocols they want to use, what security updates to apply, and any other upgrades that is essential to protect the network and system infrastructure from a breach. Another thing that the IT security can do is teach preventive procedures to HR on how to properly secure their data on their workstation and preventive measures, so they know what steps to take if their computer becomes compromised. CSC security control 1.5 and 1.6 would fall under this category. A follow-up assessment will be performed six months later, from the time the security upgrades are applied. When a follow-up assessment happens, the Port of Seattle's IT department will reanalyze the security controls they have applied and see the effectiveness of those controls. Based on the results they receive from their second assessment, if it turns out be working well as they expected than no other actions needed.

Risk Mitigated: An intruder could gain access to an access panel at the kiosk machine

The rational to the mitigation against an intruder that could gain access to an access panel at kiosk machine was decided by Oscar and I. We decided to enhance the kiosk machine and Wi-Fi security settings otherwise the information that is stored could be intercepted and read by anyone who got passed the security encryption. All the personal data would be compromised. A series of options that Oscar and I came up with was to secure the access panel of the kiosk computer with either a lock and specialized key or a key pad to the access panel. To protect kiosk's operating system and its configurations, the unused USB ports need to be disabled, harden the operating system, or add extra security measures to the kiosk booth. Anyone of these options will work and prevent an intruder from accessing the system.

For the Wi-Fi, we decided to use the highest level of encryption such as 256-bit encryption on the Wi-Fi network which would make it harder for a hacker or an adversary from being able to access the network or using the Wi-Fi as tool to hack into the network. Other methods that will help minimize risk is adding adaptive security appliance devices to the network. An adaptive security appliance device is a firewall that is applied to network which prevents an unauthorize users from accessing Port of Seattle's network resources. CSC control 1.5 and 4.8 will provide the needed protection for information systems.

The start date of implementation for adaptive security appliance devices has not yet determined, but The Port of Seattle plans to apply those security devices to their system's infrastructure sometime between the year 2019 and 2020. The department who will be handling this project is IT department and a third-party vendor that the Port of Seattle hires. Once the project is completed, an additional evaluation will be scheduled at a later date.

The Port of Seattle and a third-party vendor will review the results of the assessment and see if other areas need improvements, but if it is not critical, then no improvements are necessary.

Risk Mitigated: An intruder intercepting the Wi-Fi signal to obtain information

Many Port of Seattle employees uses Wi-Fi on their laptop to do work while they are on the go. The use of Wi-Fi has proven to be used quite frequently within the work environment. So, it was necessary to make sure that Wi-Fi signal is encrypted, so the signal could not be hacked by another individual when an employee is connected to the corporate server.

The Port of Seattle has decided that it is essential to provide the necessary encryption and certificates to their mobile workstations and devices to prevent rogue devices being able to piggy back off the connection that is connected to the corporate server. The corporate server also needs some advance security protocols to be enabled as well. One of those advance security measures can include hardening the server's operating system, have the kiosk be on separate network but be able to communicate with the server. For example, kiosk can be on one network and you have a firewall that is in between the kiosk and server (firewall monitoring two networks). Overall, you want the wireless access point to have a password and preventive measures such as denial-of-service prevention enabled, so when a denial of service attack appears the access point can still stop the attack from reaching the server.

CSC control 4.4, 4.5, 4.7, and 4.8 will help protect the server from being attacked and it will also protect the wireless access point as well.

The different ways that you protect the kiosk's Wi-Fi signal is to implement intrusion detection system or an anti-virus software and have it linked to a main computer, so if any suspicious activity occur, they can find out which kiosk is under attack. Another option is to incorporate an incident respond process, so it can at least give the computer the ability to isolate the breach and prevent it from harming the system. Security control 3.6 and 4.3 will resolve this issue.

Employee workstations need to maintain security compliant to the Port of Seattle security standards. One of the ways that this can be achieved is by making sure that each of the computers have the latest security updates, encryptions are current, disable unused USB ports, tell the user to lock their computers (show login screen), etc. These are the different methods that it can be used to prevent workstations from getting broken into. Security control 4.5, 5.6, and 5.5 will provide the necessary protection against this threat.

The start date for applying these controls can be now and the end date determined on how long each security control takes to install to each workstation in the organization. Depending on how size of the security upgrade, the project could take months or years to complete. A outside vendor would be the ones to install the necessary access controls, and the Port of Seattle's IT

security engineer department will coordinate with the vendor to ensure proper controls are properly configured and satisfies Port of Seattle's security standards.

Once a year, Port of Seattle's IT staff will have a briefing reviewing the security aspects of their system's infrastructure and any new area of concerns that may have occurred during the year. If there are no new changes that need to be address, then the organization accepts that mitigation is not required.

Risk Mitigated: Thief trying to get access to a room where locked containers are stored.
If a thief wanted to break into the locked containers, he or she could pretend to be an employee and ask where the locked containers are stored. It is possible the thief could trick an employee and learn the security procedure for entering the storage room and opening one of those locked containers.

There are a variety of ways to safeguard the locked containers and the storage room. One of those ways may include a combination safe that has a two-way authentication process to get into the safe such as a traditional rotating lock mechanism and biometric scanner. Another option is to have a secure room such as a SCIF (sensitive compartmented information facility) to transfer the safe or other locked containers to that room. CSC control 5.6 will solve the issue of a thief being able to break into the locked containers. If they do not have secure room and want one, it may take several years (2019 to 2022) to get that room built.

For file cabinets, adding a pad lock to the cabinet as an extra layer of security is an option. Other options could be to keep the file cabinet hidden in a closet or use a key card to open the file cabinet. All these options will prevent the thief from gaining access to the cabinet. The duration of applying this security control can take a few weeks to purchase the physical storage containers like a safe or file cabinet. The department that would be responsible for this type of mitigation would be building manager and IT department. The building manage is the one who would supply the file cabinet or safe and IT would handle the configuration of the biometric locks on the container. A follow-up assessment for this procedure would be assessed every few years.

The residual risk would be very low that a thief would be able break into the safe or file cabinet, especially if a biometric lock is involved. The only thing that the IT manager or team would want to assess a little more frequent is the lock system of a secure room. So, in this case, the Port of Seattle would consider this as an acceptable risk.

Reference List

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing Octave Allegro: Improving the Information Security Risk Assessment Process.* Carnegie Mellon University.

Center for Internet Security. (2015). *The CIS Critical Security Controls for Effective Cyber Defense.* Center for Internet Security.

Landoll, D. J. (2011). *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments.* Boca, Raton: Taylor & Francis Group, LLC.

Segura, O. (2018, November 7). CSC Security Control Worksheets. (J. Sanchez, Interviewer)

Segura, O. (2018, November 7). Octave Allegro Worksheets. (J. Sanchez, Interviewer)

Octave Allegro Worksheets

Worksheet 1

Allegro Worksheet 1	**Risk Measurement Criteria – Reputation and Customer Confidence**		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than ___1____% reduction in customers due to loss of confidence	____2___to __9_____% reduction in customers due to loss of confidence	More than __10_____% reduction in customers due to loss of confidence
Other:			

Worksheet 2

Allegro Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than __3_____% in yearly operating costs	Yearly operating costs increase by ___3____to ___9____%.	Yearly operating costs increase by more than ___10____%.
Revenue Loss	Less than __2_____% yearly revenue loss	__2_____to __5_____% yearly revenue loss	Greater than __6_____% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $___90,000_____ _	One-time financial cost of $___90,000_____ _ to $__150,000_____ __	One-time financial cost greater than $___150,000_____ __
Other:			

Worksheet 3

Allegro Worksheet 3	**Risk Measurement Criteria – Productivity**		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff work hours are increased by less than ___1____% for ____30___to __90_____ day(s).	Staff work hours are increased between ___2____% and ___9____% for ___90____to __180_____ day(s).	Staff work hours are increased by greater than __10_____% for ___180____to _365_____ day(s).
Other:			
Other:			
Other:			

Worksheet 4

Allegro Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated
Other:			

Worksheet 5

Allegro Worksheet 5	**Risk Measurement Criteria – Fines and Legal Penalties**		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than $_50,000_____ _are levied.	Fines between $__50,000_____and $__100,000___are levied.	Fines greater than $_100,000_____ __are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than $_100,000_____ __ are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $__200,000_____ __ and $___999,000_____ __are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $__1,000,000_____are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.
Other:			

Worksheet 6

Allegro Worksheet 6	RISK MEASUREMENT CRITERIA – USER DEFINED		
Impact Area	**Low**	**Moderate**	**High**

Worksheet 7

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	**IMPACT AREAS**
3	**Reputation and Customer Confidence**
2	**Financial**
1	**Productivity**
5	**Safety and Health**
4	**Fines and Legal Penalties**
N/A	**User Defined**

Worksheet 8

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Employee's Account information	It has employee's information such as their name, employee email address, phone number, credit card number, social security number, etc.	The employee's account information is used for various things such as HR uses that information to pay their staff members. An employee uses their account to see their earning statements and any other information that is in their account.
(4) Owner(s) *Who owns this information asset?*		
Port of Seattle		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Parking managers, Port of Seattle (HR)
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Parking technicians
	This asset must be available for __24___ hours, __7___ days/week, ___52__ weeks/year.	Information Technology Technicians. *(Employees traveling on business need access to their accounts to make last minute travel changes due*

		to circumstances beyond their control.)
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	N/A

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

✓ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Worksheet 9a

Allegro Worksheet 9a	INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)	
	INTERNAL	
	CONTAINER DESCRIPTION	OWNER(S)
1.	Database holds essential information such as how many employees work at Port of Seattle, financial, other information related to the employee. CSC Controls 1.4, 3.4, and 3.5 I have interviewed Oscar that CSC control 1.4, they scan for all the systems that are connected to the network and the network devices to makes sure that all the systems that they have are accounted for. While also making sure that there are no unknown or rogue devices being connected to their internal network. CSC controls 3.4 and 3.5, Oscar has provided me the details and procedures for remote administration of their servers and workstations, along with other network devices they use VPN software to remote into those systems.	IT Department (information security) Port of Seattle's HR members
2.	Workstations which allows employees to check-in before heading to their jobs (for airline attendants: they check-in at front desk before going to their designated airline.) CSC control 2.2 Which Oscar have stated that adding to the approved applications for those workstations will reduce the possibility of file integrity from becoming altered. By using the file integrity check tool, is to make sure the program has not been modified, where it could hinder the workstations performance and the productivity.	Sea-Tac employees Port of Seattle
3.	Kiosk machine is located at the parking area, so that employees can pay for their parking spot via credit card or cash with ease without having to figure out where they have pay at. CSC control 1.4, 1.5 and 3.1 As I went through a set of security controls with Oscar, he said that control 3.1 would be applicable which is to establish a configuration of the kiosk's operating system and its application securely. Also making sure that security updates for the machine is up to date. Along with keeping track of how many kiosk devices they have.	Port of Seattle IT Department

For security control 1.5, testing or review the authentication encryption of the kiosk to make sure that is update with the Port of Seattle's security standards.	
4. Security network that has the sensitive information traveling across the network, you want to make sure that it is secured as possible by using the highest encryption available such as 256-bit encryption. CSC control 1.5 and 4.8 At my interview with Oscar, they will test the strength of network encryption and test the network security devices that have been configured such as DMZ severs, adaptive security appliance (ASA), etc. to ensure that the network is properly encrypted and secure.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Vendor's server which holds their contractors schedule information such as what project they are currently working on, when they were assigned to that project, how long the project is going to take, etc. If the contractor is traveling the vendor will have a copy of the contractors Tertiary, which would be stored or backed-up to their organization's servers.	Vendor
2.	
3.	
4.	

Worksheet 9b

Allegro Worksheet 9b	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)	
INTERNAL		
CONTAINER DESCRIPTION		**OWNER(S)**
1. Paper or electronic copies of the information about the employees can include employee background checks paperwork, paper work for promotions, etc. would be archived in file cabinet or stored on a flash drive which would be put in a locked container (a combination safe). Employee parking information could also be included. CSC Control 5.6 Port of Seattle have enabled an encryption feature such as bit locker to protect the contents of the flash drive. Other features that they have been enable are, setting a password on the document itself or making them read-only. So, the file cannot be modified. While assessing how secure the encryption is.		Vendor, Port of Seattle
2.		
3.		
4.		
EXTERNAL		
CONTAINER DESCRIPTION		**OWNER(S)**
1. Parking vendor data center, for third party contractors, the information about the contractors (name, work hours, how long they are assigned to the project) are stored the vendor's server which can be located in the server room.		Vendor Vendor's IT security Team

2.	
3.	
4.	

Worksheet 9c

Allegro Worksheet 9c	INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)	
INTERNAL PERSONNEL		
	NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
1.	Parking managers has access to employees' information which relates to where the employees are parked at (what gate and what parking spot. (e.g Gate T, parking lot 3) CSC control 4.2 How the CSC control 4.2 will be assessed is by first figuring out what automated toll booth it is (number of the toll booth) and do a security scan of its system to see if there are any vulnerabilities then do a test of attack detection to see if the event log would detect a breach. Same applies for a group of automated toll booths, if there is a vulnerability then patch would be deployed to those booths	Port of Seattle parking Management
2.	Information Technology has access to limited personal information about the employee such as a name, badge number, etc. CSC control 3.7 In the interview, Oscar have told me that Port of Seattle uses a deploy a system configuration management tools like an Active Directory. They have implemented access restrictions such as setting access permissions to their database based on the role of the job. Some of the methods that they have use applying specific permissions to a group (financial department) via creating a group policy. For example, HR would need access to social security numbers, name of the employee, bank account number, etc. So, the IT department would set access permissions to those files or folder to HR. and everybody else who doesn't need that kind of information would have been restricted.	IT
3.	Human Resource has the most access to employees account information which can include social security numbers, account numbers for direct deposit (used to pay employees), and any other information that may be relevant.	HR

CSC Control 1.5, and 1.6 One of the ways of how to access is to see how HR protects the employees' information such as how they secure their login information, what kind of encryption they use on their computers, do they use client certificates, etc. Basically, assess to see what kind of security measures they have implemented within their organization.	
4.	
EXTERNAL PERSONNEL	
CONTRACTOR, VENDOR, ETC.	**ORGANIZATION**
1. Parking vendor has the least amount information meaning, the parking vendor would have information about the toll booths at the parking structure and may have information of about the person who is parked at the available spots (Owner's name, and license plate number of that vehicle).	Parking vendor
2.	
3.	
4.	

Worksheet 10

Allegro - Worksheet 10						
		INFORMATION ASSET RISK WORKSHEET				
Information Asset Risk	**Threat**	Information Asset	Employee's Account information			
		Area of Concern	*A disgruntled employee may release an employee's account information.*			
		(1) Actor *Who would exploit the area of concern or threat?*	Employee (disgruntled)			
		(2) Means *How would the actor do it? What would they do?*	bypass the security controls of the system by using their badge or pin number to login to the system.			
		(3) Motive *What is the actor's reason for doing it?*	Interruption			
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ✓ **Modification**	✓ **Destruction** ✓ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	CSC control 3.1 and 3.5 would be bypassed. Breaking in and compromising admin account, exploiting the server, and malware defense. Improper configuration of malware defense software. It could lead to alteration of employee's account data and possibly be released to the public.			
		(6) Probability *What is the likelihood that this threat scenario could occur?*	**√ High**	☐ **Medium**	☐ **Low**	
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*			
			Impact Area	**Value**	**Score**	
	The employees may have some serious concern of their information was to be		Reputation & Customer Confidence	high	9	

	leaked to some outside parties that is not supposed to have access.	Financial	medium	2
	If the employee's financial data was to be released or altered, it could either prevent that specific employee from getting paid or their funds vulnerable to theft.	Productivity	low	1
		Safety & Health	low	5
		Fines & Legal Penalties	low	4
		User Defined Impact Area		
			Relative Risk Score	**21**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

Accept	☐ **Defer**	✓ **Mitigate**	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Database	- Implement security controls to database and add permission controls to the files to limit the possibility of unauthorize users from gaining access to that information. - CSC Controls 1.4, 3.4, and 3.5
Workstations	- Add access controls and encryption tools to the workstations whether it is a laptop or desktop. If it is a laptop you want to encrypt the hard drive with a password and may want to add an extra layer of security when accessing financial information via web, to reduce the change of the data being intercepted. - CSC control 2.2

Worksheet 10

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Information Asset	Employee's Account information		
		Area of Concern	*A hacker may gain access to employee's account information.*		
		(1) Actor *Who would exploit the area of concern or threat?*	Adversary or a hacker		
		(2) Means *How would the actor do it? What would they do?*	Disruption of service such as denial-of services attack		
		(3) Motive *What is the actor's reason for doing it?*	To become famous or bring down the company		
		(4) Outcome *What would be the resulting effect on the information asset?*	**√ Disclosure** ☐ **Modification**	✓ **Destruction** ✓ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	CSC Control 1.5, and 3.4 How CSC 1.5 and 3.4 security controls could get bypassed is, the configuration of setting up security authentication services could have not been configured properly. Or maintenance of the system may not have taken the proper precautions as it should; such as doing frequent or periodic scans to see if the network has breached.		
		(6) Probability	☐ **High**	☐ **Medium**	✓ **Low**

		What is the likelihood that this threat scenario could occur?			

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Port of Seattle may have to do extensive risk assessment and figure out what kind of damage was done and see how bad their reputation was damaged. It may require for them to re-establish confidence with their own staff.	Reputation & Customer Confidence	medium	9
	Financial	medium	4
If a hacker was after financial records such as Port of Seattle's account and routing numbers, it could cause them to lose a lot of money. Also, may cause setbacks where they will have to hold off on what they are doing (project, upgrades, etc.).	Productivity	low	2
	Safety & Health	low	5
	Fines & Legal Penalties	low	1
	User Defined Impact Area		
		Relative Risk Score	**21**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☐ **Accept**	☐ **Defer**	✓ **Mitigate**	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Dedicated archived database	- Installing two-way authentication process using an ID badge with a chip to login and password. - A USB-based login method to gain access to the archives. - Dedicated personnel who only handles archiving old or current information that needs to be archived. - VPN software - CSC Controls 1.5 and 1.6

HR	- Have HR or financial department make sure that the financial data is secure whether it is on their workstation or backed up in a secure location. - CSC control 1.5 and 1.6

Worksheet 10

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	**Threat**	Information Asset	Employee's Account information
		Area of Concern	*An intruder could gain access to the access panel to plug in their hacking device (like keyboard or rubber ducky USB drive) at kiosk machine.*
		(1) Actor *Who would exploit the area of concern or threat?*	Adversary
		(2) Means *How would the actor do it? What would they do?*	They could pose an IT contractor and use a key to open the access panel and plug in their device to steal information that is stored on kiosk computer.

		(3) Motive *What is the actor's reason for doing it?*	Create havoc on Port of Seattle		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ✓ **Modification**	☐ **Destruction** ☐ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	CSC control 1.4, 2.3, and 3.1 Exploiting the Kiosk's system configurations via inserting commands to tell it to do something which could be downloading the stored information to a removeable drive.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	✓**Medium**	☐ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Downloading information such as credit card numbers, names of the individuals, vehicle licenses plate numbers, etc. Which could affect customers or employee's confidence about the security of the kiosk machine.	Reputation & Customer Confidence	high	9
	Financial	high	12
If the breach was to happen the cost of reconfiguring and re-securing the kiosk computer, the financial cost would be significant.	Productivity	low	2
	Safety & Health	low	5
	Fines & Legal Penalties	low	1
	User Defined Impact Area		
		Relative Risk Score	**29**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
☐ **Accept**	☐ **Defer**	✓ **Mitigate**	☐ **Transfer**
For the risks that you decide to mitigate, perform the following:			

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Kiosk machine	- Secure the access panel to the kiosk computer whether is a specialized lock and key - Disable USB ports when they are not needed. - Harden the operating system or add security measures to system configurations. - CSC control 3.1 and 3.2, and 3.6
Security Network	- Use the highest available encryption such as 256-bit encryption level. - Add adaptive security appliance devices to the network. So, it can prevent the network from being breached and the chance of the data leaking out. - CSC control 1.5 and 4.8

Worksheet 10

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	**Threat**	Information Asset	Employee's Account information
		Area of Concern	*An intruder being able to use WIFI to obtain information from the Kiosk machine.*

		(1) Actor *Who would exploit the area of concern or threat?*	Adversary		
		(2) Means *How would the actor do it? What would they do?*	Using the WIFI to connect to the internal network where the Kiosk is connected to.		
		(3) Motive *What is the actor's reason for doing it?*	Malicious intent		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ✓ **Modification**	☐ **Destruction** ☐ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	CSC Control 3.1, 3.2, and 4.2 Adversary may compromise a server or workstation where the Kiosk could be connected to the same network as the workstation, which the workstation could be used as a server. Once adversary establishes foothold then they will exploit other vulnerabilities within the host to gain elevated credentials and move laterally to gain domain credentials and continue to infiltrate the environment and establish counter measures to prevent detection.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	✓**Medium**	☐ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
If the server becomes compromised and have control of the server, it could also mean that the adversary could cause further damage to the system such as deleting files off the server. Which could cause employees to question security procedure that Port of Seattle has in place.	Reputation & Customer Confidence	high	9
	Financial	high	12
	Productivity	medium	2

	Financial records such as corporate account information can be compromised and funds from that account could become depleted.	Safety & Health	low	5
	The continuity and productivity of Port of Seattle could be reduced. Which would slow down the speed for them to get things done.	Fines & Legal Penalties	low	1
		User Defined Impact Area		
			Relative Risk Score	**29**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☐ **Accept**	☐ **Defer**	✓ **Mitigate**	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Server	- Harden the operating system - Have a separate network but have the Kiosk be able to communicate with the server. For example, Kiosk can be on one network and you can have some sort of firewall that is in between the kiosk and server (firewall could monitor two networks). - Harden the wireless access point with a password but have other preventive measures such as denial-of-service prevention enabled. - CSC Control 4.4, 4.5, 4.7, and 4.8
Kiosk machine	- Implement intrusion detection system to the kiosk machine or an antivirus software that is somehow linked to main computer or office at Port of Seattle, they know that there is something suspicious going on at the kiosk computer. - Incorporate incident response process so that the machine could at least isolate or quarantine the breach from continuing to harm that system. - CSC control 3.6 and 4.3
Workstation	- Increase security of the workstation such as using a finger print scanner. - Disable unused USB ports. - Tell users to lock their computers (show login screen) before stepping away even for a minute. - CSC Control 4.5, 5.6, and 5.5

Worksheet 10

Allegro - Worksheet 10			INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	**Threat**	Information Asset	Employee's Account information		
		Area of Concern	*A Thief trying to get access to a room where locked containers are stored.*		
		(1) Actor *Who would exploit the area of concern or threat?*	Thief		
		(2) Means *How would the actor do it? What would they do?*	Elevation of privileges by social engineering to trying find out where the locked containers are stored in the room.		
		(3) Motive *What is the actor's reason for doing it?*	Political statement		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ✓ **Modification**	☐ **Destruction** ☐ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	CSC Controls 4.1 Adversary may use social engineering to gain access to confidential data by several means such as impersonating some else or compromising user's device.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	✓**Medium**	☐ **Low**

	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
	An Unauthorize individual could get into the room where the locked container is stored and take the contents then sell it or use it as leverage.	Reputation & Customer Confidence	Medium	6
		Financial	low	2
	There could be a lawsuit against Port of Seattle for the data breach. Which Port of Seattle may have pay out money to the individual who had their identity stolen.	Productivity	low	1
		Safety & Health	low	5
		Fines & Legal Penalties	medium	8
		User Defined Impact Area		
			Relative Risk Score	**22**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☐ **Accept**	☐ **Defer**	✓ **Mitigate**	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Combination Safe	- Have a combination safe where that has a two-way method to get into a safe. For example, a safe that has a traditional rotating lock mechanism and with biometric system built-in, will help reduce the chance of the safe - Implement a secure room such as SCIF (sensitive compartmented information facility). - CSC Control 5.6
File Cabinet	- Maybe add a pad lock to the cabinet for extra security. - Keep the file cabinet hidden somewhere like in a closet. - Another locking mechanism could be a key card. - CSC control 5.6

Octave Allegro Questionnaires

In this appendix, you will find three threat scenario questionnaires, one for each of the container types in which an information asset can be stored, transported, or processed (technical, physical, and people). These questionnaires are used in Step 5 of the OCTAVE® Allegro process to help ensure a robust consideration of threats in the assessment process.

Threat Scenario Questionnaire 1	**Technical Containers**		
This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Threat Scenario Questionnaire – 1 (cont)	**Technical Containers**

Scenario 3:

In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

- Unintended disclosure of your information asset
- Unintended modification of your information asset
- Unintended interruption of the availability of your information asset
- Unintended permanent destruction or temporary loss of your information asset

A software defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A system crash of known or unknown origin occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A hardware defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Malicious code (such as a virus, worm, Trojan horse, or back door) is executed	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Power supply to technical containers is interrupted	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Problems with telecommunications occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Other third-party problems or systems	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Threat Scenario Questionnaire – 2	**Physical Containers**

This worksheet will help you to think about scenarios that could affect your information asset on the physical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.

Scenario 1:

Think about the people who work in your organization. Is there a situation in which an employee could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Scenario 2:

Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Threat Scenario Questionnaire -2 (cont)	**Physical Containers**

Scenario 3:

In this scenario, consider situations that could affect your physical containers and, by default, affect your information asset. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

- Unintended disclosure of your information asset
- Unintended modification of your information asset
- Unintended interruption of the availability of your information asset
- Unintended permanent destruction or temporary loss of your information asset

Other third-party problems occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Threat Scenario Questionnaire – 3	People		
This worksheet will help you to think about scenarios that could affect your information asset because it is known by key personnel in the organization. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee has detailed knowledge of your information asset and could, *accidentally* or *intentionally*, cause the information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?[1]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?[2]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?[3]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could, *accidentally* or *intentionally*, cause your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

[1] This case is unlikely, but if a key person in your organization has detailed knowledge of an information asset and communicates this information in an altered way that affects the organization, a risk could result.

[2] This case is about the availability of the information. If a key person in the organization has detailed knowledge that is vital for a business process and is not accessible or available, the information may not be usable for the purpose intended, ultimately impacting the organization.

[3] If a key person in the organization knows the information asset and leaves the organization, and the information is not documented elsewhere, it could pose a risk to the organization.