Risk Assessment – Asset Inventory

Seawall Security

Revision 1

Date of Publication: October 11, 2021

Seawall Security Headquarters
1234 Seawall Blvd
Galveston, TX 77554

CYBS-8396-7QA

Harrison Richardson, CISSP, OSWE
Chief Information Security Officer (CISO)

Table of Contents

Executive Summary

The first step an organization must take to improve their security posture and work to prevent cyber-attacks is to identify possible weaknesses in the company's infrastructure that could be exploited. This process is known as a Risk Assessment (ISACA, 2010). When conducting a Risk Assessment, security analysts should first perform an inventory of assets that are essential to the organization's success and assign a value to each of these assets. The asset's value should be determined based on the amount of revenue they generate, either directly or indirectly. Next, the company's internal security team must identify the tools, techniques, and methodologies that an attacker would most likely use to target each asset. This information will allow analysts to target specific vulnerabilities on these assets for remediation based on what vulnerability is most likely to be targeted. Finally, a risk mitigation strategy should be developed that identifies security controls the organization can put in place to reduce the risk of a successful attack. These controls should both decrease the chances that an attacker will successfully exploit the specific asset, as well as reduce the impact in the event that a breach does occur.

The following document details Seawall Security's Risk Assessment methodology. An asset's level of risk is defined with quantitative data derived from internally developed algorithms. All assets are given a Risk Score between zero and five hundred based on the impact of a successful attack on each aspect of the CIA Triad (Confidentiality, Integrity, and Availability). This Risk Score is then modified by applying a multiplier based on the assets value. This value is derived from the asset's impact on the company's estimated annual revenue. Once the asset's Risk Score is calculated a mitigate strategy is outlined with specific, actionable steps that can be taken by Seawall Security's internal security team to reduce the likelihood and impact of a breach. A modified Risk Score is then calculated showing the reduction of risk that will be achieved by the security controls detailed in the mitigation strategy. The security controls outlined in the mitigation strategy have also been designed to reduce the greatest amount of risk while having minimal impact to the company's operations and overhead. The goal of this document is to maximize long-term company profits by making small investments in security controls that will have a significant, long-lasting impact.

Seawall Security – Risk Assessment

Most notable cybersecurity companies today operate with a large amount of overhead. While some overhead spending on marketing or research is essential, other expenses like elaborate corporate offices and lavish parties are not. So why does that matter? It's easy for onlookers to write off these unnecessary expenses as simple company benefits that only hurts their own bottom line. Until, that is, you realize that these expenses are passed on to their customers. These increased rates are not usually an issue for organizations with millions of dollars in annual profits, but what about small businesses? Not only are cybersecurity services unaffordable for most "Mom and Pop" shops, but security vendors often won't even engage with these companies because the vendor's operating costs are so high that they will lose money from the services provided. This is where Seawall Security comes in.

Seawall Security is a new type of cybersecurity consulting company. Operating out of the Houston area, Seawall Security leverages remote workers across the United States to provide affordable security services to small businesses. In order to properly secure its client's infrastructure, Seawall Security must first defend itself against cyber-attacks. To accomplish this goal, the company's internal security and compliance teams have performed a comprehensive risk assessment. The assessment includes an inventory of valuable company assets, as well as a deep dive into the impact of exploitation and strategies used to mitigate this risk. All security controls discussed in these risk mitigation strategies are driven by the success of the business, with the goal of improving operational efficiency instead of hindering it. This concept, known as governance, is a fundamental part of Seawall Security's risk mitigation strategy. Security is, and will continue it be, directly aligned with the company's mission, vision, and economic goals.

Asset Inventory

Although cybersecurity policies can be an effective way to define the systems, processes, and goals an organization uses to protect its sensitive data, these policies are often written at a high-level with language left intentionally vague. Once the policies have been implemented, it is the responsibility of the company's internal security team to apply these standards to specific use cases. Analysts are expected to leverage various tools to identify actionable steps that must be taken to produce a measurable reduction in risk. One such tool is an asset inventory. By identifying assets that are vital to an organization's continued success, the security team can then perform a comprehensive risk assessment on these assets. This risk assessment should first identify the value of the asset itself. Next, analysts must identify a vulnerability within that asset that is likely to be exploited, as well as the impact of this exploitation. Finally, a mitigation strategy should be formulated to reduce the risk of exploitation as much as possible without effecting business operations.

It is impossible to effectively measure an asset's risk, as well as the impact of exploitation, without first understanding the financial operations of the company itself. The following equations are used to determine Seawall Security's Estimated Annual Revenue (EAR) and Estimated Daily Loss (EDL) in the event of a breach. These metrics will be used throughout the following risk assessments to quantify risk by associating it with tangible financial losses.

Variable	Real-World Value
C	Number of Consultants
AE	Average Number of Engagements (Annually)
EEmin	Minimum Estimated Earnings Per Engagement
EEmax	Maximum Estimated Earnings Per Engagement
AS	Annual Salary for Consultant

Estimated Annual Revenue (EAR) = C * AE * ((EEmin + EEmax) / 2)
Estimated Daily Loss (EDL) = (((EEmin + EEmax) / 2) * AE) / 365 + AS / 365

Seawall Security has around 50 employees, 20 of which are consultants. The average client pays between $2000 and $5000 for services. Most engagements last between 3 and 5 days. Each consultant, on average, performs 200 engagements a year. Consultants are permitted to work on up to 3 engagements at one time. Each consultant earns the company an average of $700,000 per year, or around $2000 per day. Each consultant is paid an average of $100,000 per year (including health/dental/vision insurance), or $275 per day. Using the equations listed above, we can calculate that Seawall Security generates around $14 million annually with a 25% net profit margin. Additionally, if a consultant is unable to do their job it will cost Seawall Security around $2200 per day (rounded up).

20 * 200 * ((2,000 + 5,000) / 2) = 14,000,000 (EAR)
(((2,000 + 5,000) / 2) * 200) / 365 + 100,000 / 365 = 2,200 (EDL)

With these metrics established, it is now possible to begin calculating the potential impact of a successful cyber-attack on a given asset. Using the guidelines listed in the FIPS 199 publication, the impact of exploitation is calculated for each aspect of the CIA triad and placed into one of three categories: Low, Moderate, or High. The following table was taken from the FIPS 199 and outlines the specifics of each category (*FIPS 199)*.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Although the FIPS 199 guidelines do provide more specificity when compared to general cybersecurity policies, the impact categories are still open to interpretation as they stand in the publication. It is important that risk be measured using quantitative data, not qualitative, whenever possible. With this in mind, Seawall Security measures potential losses in the event of a breach through finances and reputation. The following tables illustrate how these categories are calculated.

Financial Loss Category	Losses in Relation to EAR
N/a	Losses = $0
Low	Losses < 5% EAR
Moderate	Losses > 5% < 10% EAR
High	Losses > 10% < 25% EAR

Reputation Loss Category	Expected Loss of Reputation
N/a	Incident handled internally with no one outside of the company effected in any way
Low	Incident handled internally, effect outside the company minimal, notify victims directly
Moderate	Incident may require outside consulting to resolve, customers effected negatively, will likely lead to negative press
High	Incident requires outside consulting to resolve, customers incur significant negative impacts due to breach, incident is widely reported by press

When assessing the impact of a potential breach, the expected financial loss and resulting impact to the company's reputation is calculated individually for the confidentiality, integrity, and availability of the asset's data. The higher of the two categories will determine where the CIA aspect will be placed on the FIPS 199 table. For example, if the loss confidentiality will result in Low financial losses but a High loss of reputation, the potential impact for that assets confidentiality will be classified as High.

Once all three aspects of the CIA triad have been categorized a risk score will then be calculated based on the potential impact level. All aspects of the CIA triad are treated equally, with one exception: The risk score assigned to confidentiality will be given a 3x multiplier if the compromised data includes Personal Health Information (PHI) or Payment Card Information (PCI). The loss of data pertaining to The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS) compliances would have a much greater impact on Seawall Security's reputation and could carry fines and penalties that would exponentially increase financial losses. Using a multiplier for data associated with these compliances allows the security team to better prioritize risk based on our client's needs. The following table and equation demonstrate how the asset's risk score is calculated.

FIPS 199 Category	Category Risk Score
N/a	0
Low	5
Moderate	50
High	100 (300)

Potential Impact = (Confidentiality [* 3]) + (Integrity) + (Availability)
Asset Risk Score Range = 0 – 500

Before the asset's risk score is determined using the algorithm detailed above, analysts must first calculate the asset's value to the company. This value is derived by multiplying the amount of revenue the asset generates annually with the number of consultants that will be using a single asset. For example, a consultant's laptop is only valued using the annual revenue of one consultant. Seawall Security's internal network, on the other hand, is valued based on the revenue generated by all consultants the company employs.

Variable	Real-World Value
EAR	Estimated Annual Revenue (Company)
AAR	Asset Annual Revenue
C	Number of Consultants

Percentage of Annual Revenue (PAR) = (AAR * C) / EAR

This value classification allows the internal security team to better prioritize remediation efforts based on the importance of an asset. To represent this, a multiplier is applied to each asset's risk score based on the value classification level. This is the final step in the risk assessment process. The following table details how this multiplier is calculated.

Asset Value Classification Level	Definition of Classification Level	Asset Risk Score Multiplier
Low	Generates less than 5% of annual revenue	No multiplier
Moderate	Generates between 5% and 15% of annual revenue	Asset Risk Score * 1.25
High	Generates between 15% and 25% of annual revenue	Asset Risk Score * 1.5
Critical	Generates more than 25% of annual revenue	Asset Risk Score * 2

Modified Asset Risk Score = Asset Risk Score * Asset Risk Score Multiplier
Modified Asset Risk Score Range = 0 – 1000

As a final note, Seawall Security's risk mitigation strategy designed so that individual security controls compound with others to exponentially reduce risk. As more security controls are implemented for a specific asset, other assets are further protected as well. All risk management processes are designed around the specifications and guidelines laid out in the NIST 800-37 and 800-39 special publications and are aligned with the NIST Risk Management Framework (RMF).

Consultant Laptops

Upon being hired as a consultant for Seawall Security, employees will be issued a laptop to perform all work-related duties on behalf of the company. This device will be mailed to the individual after being configured with the necessary software. Consultants will

use this laptop to perform vulnerability scanning to their clients, as well as connect remotely back Seawall Security's internal network using a Virtual Private Network (VPN) to transmit and store client data securely.

In an effort to avoid unnecessary networking issues and introducing additional risk to customers, consultants will be expected to physically bring this laptop to their client's business and connect directly to their internal network. Once connected, the consultant will run the necessary scans to gather vulnerability data that will later be used to develop reports, remediation plans, and overall guidance for the customer. These laptops are essential for all Seawall Security consultants to provide services to their clients.

Asset Value Classification

The laptops issued to Seawall Security consultants contain all necessary tools for that employee to provide services to customers. Each consultant is issued their own device and no situation should ever arise where two or more consultants are working from a single laptop. When put in the context of annual revenue, these laptops can be valued based on the amount of revenue an individual consultant generates for the company. This value currently sits at an average of $700,000. This value accounts for an estimated 5% of Seawall Security's annual revenue, making the Asset Value Classification Level for consultant laptops Moderate.

(7000,000 * 1) / 14,000,000 = 0.05 (5%)

Revenue Generated Annually	Number of Consultants	% of Company Annual Revenue	Asset Value Classification	Asset Risk Score Multiplier
$700,000	**1**	**5%**	**Moderate**	**Asset Risk Score * 1.25**

Notable Vulnerability

When a Seawall Security consultant books a job with a client, the are required (in most cases) to physically bring their laptop to the customer's location and plug that laptop directly into their internal network. Where there are many benefits to this workflow, there is also a significant risk that the consultant's laptop will be lost or stolen. This risk is inherent with most forms of remote work and is compounded exponentially as the amount of travel increases (Behling & Wood, 2007). With this in mind, the vulnerability that poses the highest risk to employee laptops is the possibility of the device itself being lost or stolen.

Impact of Exploitation

All Seawall Security consultants are issued a Lenovo ThinkPad X1 Carbon Gen 9 laptop with 16 Gigabytes (GB) of Random-Access Memory (RAM), a 512 GB Solid State Drive (SSD), and an Intel i7 quad-core processor. Each physical device costs Seawall Security $2,000. In the event that a consultant laptop is lost or stolen, this $2,000 loss will be added to the Estimated Daily Losses (EDL) value of $2,200 per day until the laptop is replaced. The following table illustrates the expected financial impact of this loss.

Duration of Impact	Total Losses	% of Company Annual Revenue	Financial Loss Category
Day	$4,200	0.03%	Low
Week	$29,400	0.21%	Low
Month	$117,600	0.84%	Low
Year	$1,411,200	10.08%	High

Seawall Security's Information Technology (IT) team, in most cases, can replace a consultant's laptop within one week. This makes the Financial Loss Category for consultant laptops Low. Unfortunately, these devices also likely contain sensitive customer data that an attacker could easily access with possession of the device. While the impact of losing this data's integrity and availability would be classified as Low, it is very likely that the impact to a loss of confidentiality would be High. It is unlikely that these laptops would contain HIPAA or PCI DSS data because consultants are required to immediately upload all sensitive data that falls under the umbrella of these compliances to Seawall Security's internal network immediately, so the 3x multiplier will not be added. The following table represents the Potential Impact of exploitation for each aspect of the CIA triad in accordance with the FIPS 199.

CIA	Financial Loss Category	Reputation Loss Category	Potential Impact (FIPS 199)	Category Risk Score
Confidentiality	Low	High	High	100
Integrity	Low	Low	Low	5
Availability	Low	Low	Low	5

Asset Risk Score = 110
Modified Asset Risk Score = 138

Risk Mitigation Strategy

Seawall Security's internal security team will take a layered, multifaceted approach to mitigate the majority of risk associated with lost or stolen employee laptops. First, the data on the device itself must be protected. Since these devices will be running a Windows operating system, an attacker with physical access to the device could temporarily change a legitimate user's password by accessing and modifying the Security Account Manager (SAM) file (*How to reset a Windows password*). To prevent this type of attack, all employee laptops will be configured with Multi-Factor Authentication (MFA). Employees will have the option of using either an authentication app on their phone (something they have) or a fingerprint scanner to authenticate using biometrics (something they are). To add an extra layer of security, the hard drive itself will be protected using full-disk encryption with cryptographic keys stored in a Trusted Platform Module (TPM) chip in accordance with control SC-28 in revision 5 of the NIST 800-53 special publication (Joint Task Force, 2020). This control will prevent attackers from removing the hard drive from the device and accessing the data directly using forensic tools and techniques.

In the event that a laptop is lost or stolen, the employee is expected to notify Seawall Security's internal security team immediately. This expectation will be clearly defined in the company's Acceptable Use Policy (AUP) and all employees must agree to the standards outlined in this policy prior to being issued a company laptop. Upon being notified, all data on the laptop's hard drive will be deleted using remote wiping software in compliance with the NIST 800-88 special publication standards (Kissel et al., 2014). Finally, Seawall Security will purchase and maintain insurance to transfer any financial risk from the loss of devices that may occur.

Implementing this mitigation strategy will greatly reduce the risk of a lost or stolen consultant laptop. The majority of this reduction in risk is a direct result of protecting the confidentiality of data stored on the device. The following table represents the asset's level of risk after the mitigation strategy has been put into practice.

CIA	Financial Loss Category	Reputation Loss Category	Potential Impact (FIPS 199)	Category Risk Score
Confidentiality	Low	Low	Low	5
Integrity	Low	Low	Low	5
Availability	Low	Low	Low	5

Asset Risk Score = 15
Modified Asset Risk Score = 19
Reduction in Risk due to Mitigation = -119

Virtual Private Network (VPN) Tunnel

All data being transmitted between Seawall Security's remote employees and the company's internal network will be sent through a secure VPN. This is a software VPN that allows Seawall Security's consultants to protect the confidentiality of customer data by establishing a secure tunnel from an insecure network. Without a secure VPN connection, all customer data would be stored locally on the consultant's device. Not only does this increase the risk of customer data being compromised, but it would also prevent Seawall Security employees from accessing existing data from the company's internal network. Maintaining this secure VPN connection is fundamental to the success of Seawall Security's remote workers.

Asset Value Classification

Due to Seawall Security's remote work policy, the company's VPN is used by nearly all employees on a daily basis. For consultants, the VPN tunnel facilitates the secure storage of sensitive customer data, as well as the ability to collaborate with other consultants by sharing access to this data when necessary. Although, it is important to note that the company VPN is not required for consultants to provide services to clients. With this fact in mind, Seawall Security's internal analysts have valued the company's VPN tunnel at one-fourth annual revenue.

((7000,000 * 20) / 14,000,000) / 4 = 0.25 (25%)

Revenue Generated Annually	Number of Consultants	% of Company Annual Revenue	Asset Value Classification	Asset Risk Score Multiplier
$3,500,000	**20**	**25%**	**High**	**Asset Risk Score * 1.5**

Notable Vulnerability

As they travel between locations, Seawall Security consultants will often be required to transmit sensitive data of insecure networks. Using a VPN tunnel to facilitate this transmission is an effective way to protect the confidentiality of this data, but this security control can also be a "double-edged sword". Using a VPN creates a single point of failure.

If an attacker manages to gain access to a user's VPN account they could access any data stored in Seawall Security's internal network. Since techniques to target the VPN infrastructure itself would take a significant amount of effort and technical knowledge to even begin to exploit, the most likely cause of a compromised VPN account would be through the user's password. There are several ways the attacker could discover a user's password without that user's knowledge. The user could choose a password without complexity, opening their account up to a brute-force attack. Another possibility is the user chooses a complex password with commonly used words or phrases that is susceptible to a dictionary attack with mutations. Even if the user selects a complex password without any guessable words, that password could have been used in other applications that were breached. This situation was what led to the Colonial Pipeline breach in 2021 (Turton & Mehrotra, 2021). It is important that Seawall Security's internal security team creates a mitigation strategy that will protect against all these scenarios simultaneously.

Impact of Exploitation

Since Seawall Security's VPN is not a requirement for consultants to render services to clients, there would be no direct financial loss if this asset was exploited. The primary financial loss would come from time invested by the company's IT team and security team working to remediate the issue. Assuming a team of 4 engineers making an average of $100,000 annual salary ($275 per day), the Estimated Daily Losses for a breach in the company VPN is $1,100.

Duration of Impact	Total Losses	% of Company Annual Revenue	Financial Loss Category
Day	$1,100	Negligible	Low
Week	$7,700	0.0005%	Low
Month	$30,800	0.0022%	Low
Year	$369,600	0.0264%	Low

Although the financial losses of a successful attack on Seawall Security's VPN would not be significant, the impact to the company's reputation would be devastating. This VPN tunnel allows users to access the company's internal network. An attacker who successfully breached the VPN would be able to execute any Create, Read, Update, or Delete (CRUD) action on data the user has access to. The impact to Seawall Security's reputation would be significant. Not only would this data be compromised, but the attacker could modify or delete data as well, impacting the integrity and availability of that data. It is also likely that HIPAA or PCI DSS data would be impacted as well, so the 3x multiplier is appropriate. The following table represents the Potential Impact of exploitation for each aspect of the CIA triad in accordance with the FIPS 199.

CIA	Financial Loss Category	Reputation Loss Category	Potential Impact (FIPS 199)	Category Risk Score
Confidentiality	Low	High	High (3x)	300
Integrity	Low	High	High	100
Availability	Low	High	High	100

Asset Risk Score = 500
Modified Asset Risk Score = 750

Risk Mitigation Strategy

The first layer of security controls that will be implemented to reduce the risk of compromised accounts for Seawall Security's VPN is to ensure the password used has not been compromised by a prior breach. To accomplish this, unique usernames will be given to users that should not represent an account name that person has used on any other platform. Users will also be given 7 days of access to DeHashed, an online platform that allows users to scrape the Dark Web for usernames and passwords that have been compromised (*DeHashed*). Upon creation of a VPN account, the hash value of the user's password will be generated using the Secure Hash Algorithm 2 (SHA256). Once generated, this hash value will be automatically compared to a list of SHA256 hash values generated from compromised password lists contained in the SecLists repository, with priority given to the new version of rockyou.txt, a widely distributed list of compromised passwords (Shaheer, 2021).

In the event that an attacker can circumvent these controls and compromise a user's VPN account password, Multi-Factor Authentication (MFA) will also be required to establish a secure connection. Employees must use an authentication application on their smart phone for MFA. At the time of writing, Seawall Security's preferred solution is Okta. Implementing MFA will prevent at attacker from accessing the company VPN even if the attacker is able to compromise a user's account. Finally, Seawall Security's internal security team will implement a Security Information and Event Management (SEIM) tool to monitor VPN connections and traffic. This SEIM must include some form of User Behavior Analytics (UBA) that recognizes and generates alerts if a user demonstrates unusual behavior such as logging in at unusual times or places. This will give Seawall Security's internal security team the ability to respond if a sophisticated attacker manages to bypass all other security controls.

These mitigation techniques greatly reduce the chances of a successful breach on the company VPN. Furthermore, by implementing reactive controls with the use of a SEIM w/ UBA it is very likely that a successful attack would be identified and contained before data was significantly compromised. The following table illustrates the potential impact of a compromised VPN once the mitigation strategy has been implemented.

CIA	Financial Loss Category	Reputation Loss Category	Potential Impact (FIPS 199)	Category Risk Score
Confidentiality	Low	Moderate	Moderate (3x)	150
Integrity	Low	Low	Low	5
Availability	Low	Low	Low	5

Asset Risk Score = 160
Modified Asset Risk Score = 240
Reduction in Risk due to Mitigation = -510

Customer Data

Seawall Security offers a wide range of services for its customers. Some examples are vulnerability management assessments, penetration tests, and white-box application code reviews. In order to provide these services, consultants must gather a significant amount of sensitive information from their clients. Protecting this data is Seawall Security's number one priority. A breach resulting in loss of customer data would not only do irreparable damage to the company's reputation but could open the company up to legal action and financial consequences. All aspects of the CIA triad are important when dealing with customer data. The confidentiality must be preserved to protect the client's privacy, as well as honor any Non-Disclosure Agreements (NDAs) that may be in place. The integrity

must be maintained to ensure accurate guidance is provided to the client. Finally, the customer data must be available at all times to ensure Seawall Security's consultants can provide services in an effective and timely manner.

Asset Value Classification

There is no way around the fact that the services Seawall Security provides its clients are entirely reliant on the customer's data. This data drives 100% of the company's annual revenue and should be valued accordingly. Without customer data there is no business to protect.

(7000,000 * 20) / 14,000,000= 1 (100%)

Revenue Generated Annually	Number of Consultants	% of Company Annual Revenue	Asset Value Classification	Asset Risk Score Multiplier
$14,000,000	**20**	**100%**	**Critical**	**Asset Risk Score * 2**

Notable Vulnerability

The mitigation strategies implemented for employee laptops and the company's VPN tunnel will go a long way to prevent the loss of sensitive customer data, but when considering the data itself the most likely attack method cyber criminals will employ is social engineering (Alkhalil et al., 2021). Attackers will likely use a combination of Open-Source Intelligence (OSINT), along with phishing and vishing attacks that leverage email and phone calls respectively to convince a Seawall Security employee to voluntarily provide sensitive information. Social engineering is one of the most common methods attackers use against private companies because the attacks take minimal effort and have a high success rate. Protecting against social engineering attacks will be essential to maintain trust with customers and protect Seawall Security's reputation.

Impact of Exploitation

Calculating the financial loss of customer data can be very difficult. There are a lot of variables that need to be considered before an accurate number can be determined. As was discussed in the Asset Value Classification section, the value of the data itself is equal to the company's revenue. Since the company is unable to function in any capacity without customer data, these losses will be compounded with the company's operating expenses. Taking Seawall Security's 25% net profit margin into consideration, the financial consequences of a cyber-attack that compromises customer data will be calculated as the loss of revenue for all 20 consultants with a 1.75x multiplier.

Duration of Impact	Total Losses	% of Company Annual Revenue	Financial Loss Category
Day	$70,000	0.5%	Low
Week	$490,000	3.5%	Low
Month	$1,960,000	14%	High
Year	$23,520,000	168 %	High

It is highly likely that loss of all customer data would take weeks to recover. As a result, the Financial Loss Category for customer data will be set as High. There is also a

high possibility that a breach resulting in the loss of confidentiality or availability for this data could lead to significant damage to the company's reputation and should be listed as High as well. The Integrity, however, can be classified as Moderate for loss of reputation as this would only impact our consultant's ability to provide services effectively by advising based on erroneous data. It is also very likely that HIPAA or PCI DSS data will be involved so the 3x multiplier must be used.

CIA	Financial Loss Category	Reputation Loss Category	Potential Impact (FIPS 199)	Category Risk Score
Confidentiality	High	High	High (3x)	300
Integrity	High	Moderate	High	100
Availability	High	High	High	100

Asset Risk Score = 500
Modified Asset Risk Score = 1000

Risk Mitigation Strategy

Social engineering is a notoriously difficult attack vector to defend against. With this in mind, Seawall Security will implement a combination of technical controls and education to help reduce the risk posed by successful social engineering attacks. Beginning with the technical controls, an enterprise email security tool like Mimecast will be leveraged to identify potential phishing emails and ensure those emails do not reach users in the first place. The Principle of Least Privilege will also be used when implemented access controls for all users to ensure if a user's account is compromised the impact of this breach will be limited. Unfortunately, there are several techniques attackers can use to circumvent these filters. Continuous education and ensuring security awareness a vital part of the company culture will be paramount in the fight against social engineering.

To start, employees will receive quarterly training on modern phishing attacks and the correct way to respond if they are targeted. Employees must also review and agree to Seawall Security's Email Security Policy prior to being given a corporate account. To help ensure the skills outlined in the training and policy are not being forgotten, the company's internal security team will carry out phishing campaigns to identify employees who may easily fall victim to social engineering attacks. Employees who fail to follow proper protocols as a result of these internal campaigns must complete additional security awareness training and could possibly face disciplinary action for repeat offenses.

Finally, a comprehensive Incident Response Plan (IRP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) will be built and implemented to ensure if customer data is compromised or lost in any way the availability of this data can be returned within 3 days. The combination of security controls implemented to protect the consultant laptops and company VPN compounded with these security controls, the risk of a successful attack is greatly reduced. Furthermore, the use of planning and policies to enable Seawall Security's internal security team to respond effectively in the event of wide-spread data loss will significantly limit financial losses if an attack is successful.

CIA	Financial Loss Category	Reputation Loss Category	Potential Impact (FIPS 199)	Category Risk Score
Confidentiality	Low	High	High (3x)	300
Integrity	Low	Moderate	Moderate	50
Availability	Moderate	Moderate	Moderate	50

Asset Risk Score = 400

Modified Asset Risk Score = 800
Reduction in Risk due to Mitigation = -200

Company's Internal Network

Once data has been collected from customers it should immediately be transmitted to Seawall Security's internal network (over a VPN connection) where it can be stored and maintained securely. This process can only be successful if the company's internal network always remains available and secure. If the network were to become unavailable, Seawall Security's remote workers and consultants would be forced to store sensitive data on their company laptop. Not only would this increase the risk of a data breach, but employees would be unable to share sensitive data with others who need it and may lead to employees using insecure data transmission methods out of desperation. Furthermore, if this network were to be breached, an attacker could access a wealth of sensitive information including trade secrets, customer data, and employee Personal Identifiable Information (PII). Seawall Security's internal network is the backbone of the company's operations.

Asset Value Classification

The value of Seawall Security's internal network is calculated using an almost identical methodology to the company's VPN. While this network does help facilitate the services offered to customers, Seawall Security's consultants can still provide those services without access to this network. With this in mind, the company's internal network is valued at one-fourth of the Estimated Annual Revenue.

((7000,000 * 20) / 14,000,000) / 4 = 0.25 (25%)

Revenue Generated Annually	Number of Consultants	% of Company Annual Revenue	Asset Value Classification	Asset Risk Score Multiplier
$3,500,000	**20**	**25%**	**High**	**Asset Risk Score * 1.5**

Notable Vulnerability

Seawall Security's internal network is designed so that it can only be accessed through a VPN connection. Outside of connections through a secure tunnel, the network itself is air gapped. This architecture will prevent attackers from targeting the network itself through logical connections but opens the risk of being targeted physically. If an attacker were to gain access to the facility housing the data storage servers they could connect to the internal network directly. This breach would compromise the confidentiality, integrity, and availability of all data stored in Seawall Security's internal network. Physical security controls must be implemented to prevent an unauthorized individual from accessing the facility.

Impact of Exploitation

Just like when calculating the value of the company's internal network, the impact of exploitation to this network is nearly identical to the financial and reputation losses Seawall Security would incur if the VPN tunnel was successfully breached, resulting in financial losses of $1,100 per day and a significant impact to the company's reputation.

Duration of Impact	Total Losses	% of Company Annual Revenue	Financial Loss Category
Day	$1,100	Negligible	Low
Week	$7,700	0.0005%	Low
Month	$30,800	0.0022%	Low
Year	$369,600	0.0264%	Low

CIA	Financial Loss Category	Reputation Loss Category	Potential Impact (FIPS 199)	Category Risk Score
Confidentiality	Low	High	High (3x)	300
Integrity	Low	High	High	100
Availability	Low	High	High	100

Asset Risk Score = 500
Modified Asset Risk Score = 750

Risk Mitigation Strategy

Although it's often overlooked, physical security can be just as important as logical security. Seawall Security's risk mitigation strategy for attackers gaining physical access to the company's internal network begins by assuming the attacker is successful. With this in mind, the layers of security will be implemented from the inside out. If an attacker does gain access to the facility, they will likely attempt to connect through an open ethernet port. To prevent this, all open ports in the facility must be disabled if they are not in use. When the attacker recognizes this, it can be assumed that they will move on to an ethernet port that is currently in use by unplugging the cable and using their own. Any loss of connection within Seawall Security's internal network will immediately trigger an alert that will be sent to Seawall Security's internal Security Operations Center (SOC) analysts. The SOC analysts can then compare the disconnection event with the company's change management documentation to quickly identify if this event was planned. In the event of an unplanned disconnection, the SOC analyst will disable that port remotely to prevent any data loss that may occur.

While these controls will be an important part of protecting Seawall Security's internal network, the goal is to ensure attackers are never able to physically enter the facility in the first place. In an effort to accomplish this, guards will be posted at the only entrance/exit to the facility at all times. Security cameras with motion sensing technology will also be installed both inside and outside the facility. Any unexpected motion will immediately trigger an alert to the SOC team. Finally, authorized employees must use Multi-Factor Authentication (MFA) to access the facility. This MFA will take the form of a smart card with a chip and a fingerprint scanner. Radio-Frequency Identification (RFID) will not be used due to the risk of compromise using an RFID cloner being too great (Li et al., 2015).

The benefits of the security controls detailed in this risk mitigation strategy are, again, like the benefits of securing the company's VPN tunnel. There is, however, one major exception. If an attacker does gain physical access to the facility and connects to Seawall Security's internal network, the risk to the availability of the network will be higher than the risk of connecting through a compromised VPN. With this in mind, the potential impact of a successful breach on the company's internal network will be classified as Moderate.

CIA	Financial Loss Category	Reputation Loss Category	Potential Impact (FIPS 199)	Category Risk Score
Confidentiality	Low	Moderate	Moderate (3x)	150
Integrity	Low	Low	Low	5
Availability	Moderate	Moderate	Moderate	50

Asset Risk Score = 205
Modified Asset Risk Score = 308
Reduction in Risk due to Mitigation = -442

Data Storage Servers

All data transmitted to Seawall Security's internal network is stored on a collection of physical servers. These data storage servers allow remote employees to securely store and access client data. Just like with the company's internal network, the loss or compromise of these servers would greatly increase the risk of a data breach and prevent effective data transmission between remote employees. All aspects of the CIA triad must be protected for Seawall Security to operate successfully.

Asset Value Classification

Seawall Security's data storage servers are valued using the same methodology and reasoning as the company's VPN and internal network.

((7000,000 * 20) / 14,000,000) / 4 = 0.25 (25%)

Revenue Generated Annually	Number of Consultants	% of Company Annual Revenue	Asset Value Classification	Asset Risk Score Multiplier
$3,500,000	**20**	**25%**	**High**	**Asset Risk Score * 1.5**

Notable Vulnerability

At this point the mitigation strategies implemented will go a long way to protect Seawall Security's data storage servers, but there is one attack vector that has not been addressed: supply chain attacks. There servers used in the company's internal network, as well as some software running on those servers, must be purchased from vendors. It is possible for those vendors to have their supply chains compromised, leading to backdoors or malware being implanted in the device before Seawall Security purchases and installs it. The devastating impact of this type of attack was made clear in December of 2020 when a similar attack was carried out successfully against SolarWinds, leading to the compromise of over 300,000 customers, including United States government agencies and 425 of the US Fortune 500 companies (Williams, 2021).

Impact of Exploitation

In the event that an attacker can successfully execute a supply chain attack on Seawall Security's data storage servers, that device must immediately be removed from the company's infrastructure and replaced as soon as possible. This means the financial losses

that will result from a successful exploit can be measured as a one-time cost for the device itself. The average storage array the company purchases is around $50,000 per unit.

Duration of Impact	Total Losses	% of Company Annual Revenue	Financial Loss Category
One-Time	$50,000	0.36%	Low

Although the financial losses of such an attack will not be significant, a successful supply chain attack could be devastating to the company's reputation. Supply chain attacks require a highly sophisticated, coordinated effort and are most commonly executed by a well-funded and/or state-sponsored hacker group (McAfee, 2021). These groups often used Advanced Persistent Threat (APT) techniques that are incredibly difficult to detect. The impact of a successful supply chain attack would be devastating to Seawall Security's reputation and should be measured accordingly.

CIA	Financial Loss Category	Reputation Loss Category	Potential Impact (FIPS 199)	Category Risk Score
Confidentiality	Low	High	High (3x)	300
Integrity	Low	High	High	100
Availability	Low	High	High	100

Asset Risk Score = 500
Modified Asset Risk Score = 750

Risk Mitigation Strategy

Supply chain attacks are one of the most difficult types of attacks to defend against, but there are methods to reduce risk. Seawall Security will leverage security ratings given to third-party vendors and conduct annual Third-Party Risk Management (TPRM) assessments to mitigate some risk associated with these attacks. Guidelines outlined in the NIST publication *Defending Against Software Supply Chain Attacks* will also be followed when purchasing any third-party software that will later be installed on Seawall Security's data storage servers. Unfortunately, there is a certain level of risk that must be accepted with this attack vector. Instead of working to prevent these attacks all together, Seawall Security's internal security team will ensure that if a breach does occur they can quickly identify the attack and greatly reduce the impact caused by the incident.

While this mitigation strategy can help prevent supply chain attacks, there is simply no way to guarantee that malicious insiders have not infiltrated the supply chain. Security controls can be used to reduce the impact to data integrity and availability but the risk to confidentiality remains High.

CIA	Financial Loss Category	Reputation Loss Category	Potential Impact (FIPS 199)	Category Risk Score
Confidentiality	Low	High	High (3x)	300
Integrity	Low	Moderate	Moderate	50
Availability	Low	Moderate	Moderate	50

Asset Risk Score = 400
Modified Asset Risk Score = 600
Reduction in Risk due to Mitigation = -150

References

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021, January 1). *Phishing attacks: A recent comprehensive study and a new anatomy*. Frontiers. Retrieved October 8, 2021, from https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full.

Behling, R., & Wood, W. (2007). Laptop theft: A growing concern for organizations. *Issues In Information Systems*. https://doi.org/10.48009/2_iis_2007_291-296

DeHashed. (n.d.). Retrieved October 8, 2021, from https://www.dehashed.com/.

How to reset a Windows password. Ethical hacking and penetration testing. (n.d.). Retrieved October 8, 2021, from https://miloserdov.org/?p=4287.

ISACA. (2010, January 1). *Performing a security risk assessment*. Performing a Security Risk Assessment. Retrieved October 12, 2021, from https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment.

Joint Task Force. (2020, September). Security and Privacy Controlsfor Information Systems and Organizations. Retrieved October 8, 2021, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014, December). *Guidelines for media sanitization - NIST*. Guidelines for Media Sanitization. Retrieved October 8, 2021, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

Li, P., Xu, C., Chen, L., & Wang, R. (2015). RFID privacy risk evaluation based on synthetic method of extended attack tree and information feature entropy. *International Journal of Distributed Sensor Networks*, *11*(11), 146409. https://doi.org/10.1155/2015/146409

McAfee. (2021, April). *McAfee Labs Threats Report, April 2021 - HSDF*. McAfee Labs Threats Report. Retrieved October 12, 2021, from https://www.hsdf.org/wp-content/uploads/2021/06/rp-quarterly-threats-apr-2021.pdf.

Shaheer. (2021, June 9). *Rockyou.txt (ROCKYOU2021) password list download (latest)*. SecuredYou. Retrieved October 8, 2021, from https://www.securedyou.com/rockyou-txt-rockyou2021-download/.

Turton, W., & Mehrotra, K. (2021, June 4). *Hackers Breached Colonial Pipeline Using Compromised Password*. Colonial Pipeline Cyber Attack: Hackers Used Compromised Password - Bloomberg. Retrieved October 8, 2021, from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

U.S. DEPARTMENT OF COMMERCE. (n.d.). *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199. Retrieved October 10, 2021, from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

Williams, J. (2021, September 30). *What You Need to Know About the SolarWinds Supply-Chain Attack*. What You Need To Know About the SolarWinds Supply-Chain Attack | SANS Institute. Retrieved October 8, 2021, from https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/.