Information Assurance Plan for a Retail Company

Brett Logan

Southern New Hampshire University: Global Campus

IT 549: Foundation in Information Assurance

Professor: R. Lopez

April 22, 2021

Table of Contents

Table of Contents (cont.)

I. Information Assurance Plan Introduction

a. Overview of Goals and Objectives

As one of the major constituents of the retail industry here in the U.S., this company has a duty to protects its customers, employees, and shareholders. A key piece of this protection is the proper recognition of the importance of information security (infosec): "a process of preventing unauthorized access, counter threats, confidentiality, disruption, destruction, and modification of business data" (Costa 2019). This is where the adoption of a well-crafted information assurance plan comes into play, one that aims to keep all data within the enterprise operations safe and protected, in line with legal and ethical norms and ongoing security protocols. At the end of this plan, stakeholders will understand how it benefits them and the company as a whole, and why the adoption and implementation of it is the right course of action. The information assurance plan seeks to achieve the following goals and objectives:

-Maintain the *confidentiality* of sensitive information gathered through business operations, customer transactions, and data processing/storage.

-Ensure the *integrity* of data within the business by creating and maintaining a system wherein it is possible to prove information has not been manipulated, identify the responsible party for any changes made to data, and eliminate the potential for repudiation.

-Ensure the *availability* of data and information systems at all times, including in crisis such as during a cyberattack, systems error, or natural disaster.

Together, these three objectives make up what is known as the CIA triad, and "in this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people" (Chai 2021). The importance of CIA

within our organization is critical because failing to meet this triad means failing to protect customer data, failing to adhere to laws and regulations, and the potential for network disruption and cessation of business operations altogether.

The creation and maintenance of this plan around these key concepts will lead to a stronger, better prepared organization that is equipped to prevent security breaches, and respond appropriately when necessary. Adherence to the plan will ensure continued operability and business functionality, ultimately leading to a more prosperous company and healthier bottom line, resulting in continued growth and success over the coming years.

b. Confidentiality, Integrity, and Availability of Information

Confidentiality at is core addresses the prevention of information being accessed by unauthorized users. In this organization, the most common type of information includes customer personal protected information (PPI) such as names, email addresses, postal addresses, and credit card information which is collected when customers place orders online or in-store. “It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories” (Chai 2021). This means attributing high priority to PPI such as credit card numbers, and ensuring their confidentiality through steps such as the utilization of encryption when that data is created, collected, transmitted, processed, or stored.

Data integrity in the retail industry is important to ensure efficient and uninterrupted business operations : “one of the most typical inconsistencies we can find in retailers' data is in the code on a packaging not matching the item. The packaging and labeling is still, in most cases, a human process so that many errors can occur during it. Then, the domino effect occurs when a

retailer's inventory replenishment systems use the wrong code to order the faulty product" (Feliu 2021). This example highlights the need for integrity and the importance of being able to identify parties responsible for data changes. Another effective component of a plan that ensures integrity via non-repudiation is the use of hashing, "cryptographic hash functions may be used to establish the integrity of transmitted documents. No encryption keys are involved, and strong hash functions are designed to be irreversible" (Finjan 2017). This is especially applicable to sensitive data transmitted between organizational leadership and/or management that could lead to severe operational repercussions if tempered with or altered in transit.

Finally, "organizations rely on data to deliver products and services to their customers. To keep their data "live" or "online", organizations need to keep the Information Technology (IT) infrastructure active even in the case of a disruption to the network. This state of guaranteed access to data is known as data availability" (Cloudian 2021). For example, host server failure could result in inventory data being unavailable and the interruption of sales until proper inventory numbers are back up. This could have a negative effect on sales, customer satisfaction, and brand reputation. Key priorities to prevent such an occurrence and ensure data availability include data redundancy (storing backups or utilizing a distributed network), data loss prevention tools, and erasure coding: "erasure coding combines data with parity information and then splits or "shards" it and distributes it across the storage environment. This protects against component failure as you only need a subset of the shards to restore the data" (Cloudian 2021).

These three components that make up CIA are not mutually exclusive and instead work together to contribute to the overall information security of the company. An additional note of importance lies in the ongoing shift to online shopping, especially as a result of the 2020 Covid-

19 pandemic. The organization's online storefront contributes to the creation of even more customer data, which "poses challenges to the CIA paradigm because of the sheer volume of information that organizations need safeguarded, the multiplicity of sources that data comes from and the variety of formats in which it exists" (Chai 2021). It is only through a proper and well-envisioned plan that we may address this and continue keeping both customer and corporate data safe.

c. Current Protocols and Policies

An effective example of the type of security failure a retail company like ours is vulnerable to can be illustrated via the Target data breach in 2013 in which "more than 70 million credit card numbers, addresses, phone numbers, and other personal information, were in the hands of hackers in Russia... multiple communication breakdowns and negligence led to the biggest retail security breach in U.S. history, a 46% decline in sales for the 2013 holiday season, and more than 90 lawsuits from customers and banks" (Marks 2014). Such a devastating breach could have been prevented by having the proper protocols and policies in place. Our company currently has the following policies:

-Password best practices for administrative employees (length and character stipulations, regularly mandated changes). While it may seem counterintuitive, requiring employees to change their login credentials too often can result in decreased security, and according to the Federal Trade Commission (FTC), "users who know they will have to change their password do not choose strong passwords to begin with and are more likely to write their passwords down" (Cranor 2016).

-In-store device accessibility. Currently, any customer can see screens at checkout stations and access unmanned computers at counters such as the electronics department. While

most cyber-security threats are thought of as external, an attacker could access and/or infect the company network easily through the USB drives located at these areas. Physical controls should be implemented to prevent this.

-Reliance on a central firewall. Any single point of potential failure is a weakness. The company should effectively segment the network into groupings based on department and job function, effectively creating stopgaps that could help prevent the spread of malware and protect data.

-Employee security awareness training. Currently there is no company-wide security training that focuses on common security situations employees may face such as phishing attempts and malicious email links. While implementation cost is a barrier to establishing this protocol, it could help prevent the next large scale security breach.

-Overall corporate security culture. Information assurance is not included in the mission statement. Incorporating it into the organizational culture can ensure that security awareness and preparedness increases from top to bottom. The barrier to this is cost, and convincing executive management and board members of the extreme importance of effective information assurance, which this plan will strive to do. Overall, the cost of a security breach far outweighs the cost to implement the necessary changes in protocol and policy

Barriers to Implementation

Among the greatest barriers to the implementation of this IAP is the lack of employee education and training. Once all company employees understand and comprehend the vast amount of information security risks that face us as a company, they can then understand how it affects them and their job. The best way for security to be taken seriously and the plan properly

implemented is to ensure that everyone involves feel they have a stake in its success. This can and will be achieved via training as outlined in the following plan.

II. Information Security Roles and Responsibilities

a. Responsibilities of Key Leaders

Securing information is vital to the overall success and continuity of operations within any organization. The ongoing adoption and evolution of information technologies (IT) has rapidly redesigned how a business can function, and what capabilities exist to meet corporate goals: "IT allows for more precise, feasible, robust, efficient, and streamlined business workflows, operations, and processes, along with allowing a company to offer new/better products and/or services...with the advent of cloud systems, blockchain technology, Artificial Intelligence (AI), and Big Data/Business Intelligence, new ways to increase efficiency, reduce overhead, enhance productivity, and create new products/services have become possible" (CIO 2018). Just as important and influential as IT capabilities, so too is the security of that IT. In this organization we have a security hierarchy that encompasses multiple roles and departments. Viewed from the top down, the roles of these key leaders effectively to guide all departments and employees in an effort to shield the organization from security threats and ensure uninterrupted business practices and legal compliance. Taking a closer look at some of the key leaders and their responsibilities we find the following:

Chief Information Officer (CIO):

The CIO is the senior-most IT executive and reports directly to the CEO. It is the CIO's responsibility to create and direct the overall IT strategic plan for the organization, effectively setting the security posture that will inform the actions and goals of all other personnel: "CIOs will often craft the IT strategic plan of a company, which parallels the overall business plan of

the enterprise, while also crafting IT policies, managing task automation workflows, managing the IT systems needed for data analysis, crafting plans for IT innovation, and much more" (CIO 2018). This strategic plan will contain the blueprints to ensuring information assurance.

Chief Information Security Officer (CISO):

The CISO is the senior-most cybersecurity executive within the organization. Due to the rapidly evolving threat of cyberattack and the importance of increasing regulatory compliance, the CISO will now also report directly to the CEO. While the CIO sets the strategic IT plan stipulating how IT can help achieve company objectives, the CISO protects and defends the organization's resources from security threats: "The CISO is also likely to be held accountable for security shortcomings. But when united, these IT executives can consolidate their power to have a greater say in the boardroom when it comes to technology initiatives and guiding the business" (Samuels 2020). The CISO is responsible for defending the network and thus safeguarding data.

Chief Risk Officer (CRO):

The CRO is responsible for the macro view of total operational risk management. The CRO is included here due to the extreme importance of adhering to ongoing regulations. Adherence to these regulations entails maintaining a robust and well-envisioned data security posture and policy, making the CRO role pivotal in ensuring information security. Additionally, the nature of risk analysis and the results rendered will lend further credence to the importance and impact of this information assurance plan to the organization. In order to provision the necessary funding for the IAP, we must be able to demonstrate cost-benefit of IT and Cyber investment to the board, which the CRO will play an integral part of.

Vice President of IT (VPIT):

The VPIT reports to the CIO and implements executive directives amongst employee teams with a focus on the following groups and their relative managers:

Operations: Physical IT infrastructure.

Quality Assurance: Software testing and maintenance of the online storefront to increase performance, reduce downtime, and maintain data privacy.

Vice President of Cyber Security (VPCS):

This position reports to the CISO and is responsible for the communication and implementation of security policies amongst employees. A key feature of this role is the administration of company-wide security training. Types of employees reporting to the cyber security manager will include penetration testers and security/compliance specialists.

It is noted that the key information security leadership within this organization is suggested to be heavily weighted at the executive level, a purposeful move to account for the rising importance of information assurance and how business is conducted. The internet age has moved a large portion of retail operations online, creating entirely new avenues of attack and security vulnerabilities. It is determined that the most effective and lasting way in which we can account for this is to incorporate security into the leadership of the company in ways which result in a shift in overall corporate culture resulting in integration of security throughout all departments. Doing so ensures that as online business continues to increase alongside avenues of

customer/data interaction, we as a company will be fully prepared to protect that data, our customers, stakeholders, and employees today and well into the future.

b. Key Ethical and Legal Considerations

The aforementioned leadership of this organization must take into account key ethical and legal considerations as they relate to operations and security. Such considerations include privacy, data gathering, security liability, and regulatory compliance.

Ramifications for failing to acknowledge these issues include severe financial penalty, as well as disruption of operations and loss of customers. It is the responsibility of key leadership to maintain focus on these considerations, often by working together and interweaving them into overall security posture and policy.

For example, as a retail organization engaging in online sales, this company has access to a multitude of customer data such as names, email addresses, credit card numbers, etc. Careful analysis should occur, and consideration be given to how this data is collected, processed, stored, and secured. As related to the key leadership roles, the CIO is responsible for directing what IT infrastructure will be used to harness and utilize this data in operations, the CISO is responsible for protecting the data from security threats such as hackers or malware, and the CRO is responsible for ensuring that all of the decided upon practices above adhere to regulations and limit potential risk to the organization.

There are multiple regulations that affect data and how companies interact with it, and our company is legally bound to comply. Pertinent examples include:

The European Union's General Data Protection Regulation (GDPR)

Article 32, Section 2 of the GDPR stipulates: "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised [*sic*] disclosure of, or access to personal data transmitted, stored or otherwise processed" (GDPR 2021). To accomplish compliance the CISO and CRO will need to work closely with another, further highlighting how the interaction of key leadership contributes to overall information security. It will be up to the CRO to determine the level of risks, and for the CISO to craft and implement the best security measures to protect from the risk and ensure compliance with the GDPR. Once these policies and strategies are decided upon, the VPs and managers can proceed with implementation amongst employee teams. Failure to do so "could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher" (GDPR 2021). These numbers tend to pale in comparison to the type of funding our leadership will request in order to ensure compliance and effective information assurance.

California Consumer Privacy Act (CCPA)

"The CCPA applies to any company that operates in California and either makes at least $25 million in annual revenue, gathers data on more than 50,000 users, or makes more than half its money off of user data" (Edelman 2020). As a retail company akin to Target or Walmart, the CCPA is applicable to this organization based on both brick-and-mortar and online storefronts. It "allows consumers to ask companies for the details of the personal information that the companies have collected about them or shared with third parties, and to ask for that information to be deleted" (Korolov 2020). In order to comply, we must have a developed policy that

pertains to how our customer data is gathered and stored. The CIO will be responsible for crafting this policy, and the CISO will be responsible for ensuring the cyber security of all data.

The significance of successful ethical and legal consideration extends far beyond avoiding fines and penalties. For example, a large-scale data breach, like Target has faced in the past, could cripple the ability of our organization to reach profit and maintain smooth operations. Additional effects of such breaches are loss of reputation and decreased sales due to dropping consumer confidence, especially in light of the high visibility and impact of such breaches. Having the appropriate funding and leadership can help prevent and/or mitigate events such as these.

c. Key Components of Information Assurance

Having explained the needs of our organization, it is now helpful to relate just how the key leadership roles will contribute to the core components of information assurance: confidentiality, integrity, and availability of information throughout our retail operations.

Confidentiality:

One example of how we will ensure the confidentiality of sensitive data is via the use of encryption. This decision, as well as which encryption algorithm to choose, would come from the CIO as part of the overall IT security strategy. It would be up to the VP of IT to direct the implementation of and ongoing proper use of the appropriate encryption methods among management and employees. Our CISO would be tasked with ensuring the safety and security of private keys, as well as network monitoring and the safeguarding of all encrypted data which will be accomplished through the cyber security VP and related managerial staff.

Another aspect of confidentiality is device management. The CISO should choose the appropriate cyber security hygiene practices while the cyber security VP can be tasked with ensuring enforcement among employees. The CRO might choose to audit these practices to ensure regulatory compliance and undertake risk analysis planning.

Integrity:

User access controls are a key component of ensuring the integrity of information within our systems. It is recommended that a form of identity and access management (IAM) is utilized to define job roles and limit employee access to pre-configured information zones. At the executive level, the CIO will dictate that IAM be incorporated in policy and the CISO will be tasked with the choice of software solution as well as ensuring network traffic does not indicate lapses in security. Both of these leaders will rely on VP and managerial roles to ensure no employees have access to, or the ability to change, information that they are not authorized to. Part of the cyber security team's network monitoring should include log management, and the dedicated IT team should focus on backup and recovery procedures, as well as error detection software.

Availability:

As a retail company engaging in e-commerce, it is imperative that the organization's network remain online and reliable. In today's world of increasingly sophisticated and brazen cyberattacks, hackers may attempt to disrupt network traffic (and thus the ability for our company to engage in business) via malware, DDoS attack, or other methods. The key leadership outlined above can prevent or mitigate this in the following ways:

CIO: Shall dictate that information security is a core component of the overall organizational culture, instilling best practices and training from the top down, as well as ensuring that the company has the best physical network components possible to protect information systems.
CISO: Shall create cyber security best practices and protocols to be implemented, as well as ensure all policies are remaining effective, being followed, and enforced.
CRO: Shall evaluate the overall risk to operations should hackers achieve successful data breach or discontinuity of operations. The CRO can also advise risk management solutions to be best incorporated by the CISO.
VPIT: Shall oversee offsite data backups, monitoring, and environmental controls.
VPCS: Shall enforce all cyber security protocols and act as a communication liaison between lower-level management/employee teams and executive management. The VPCS will also oversee our penetration testing team due to the sensitive security nature of any network weaknesses or issues that might be discovered.

As can be seen, the correct leadership and roles/responsibilities will play a significant part in avoiding financial losses/penalties, as well as ensuring continued profitable business operations. Especially as it relates to the increasing number of online sales, data security is only going to become more important: “Ecommerce businesses have a lot of potentials and 265% growth rate, from $1.5 trillion in 2015 to $5.9 trillion in 2023” (Kumar 2021). Implementing these key leaders now will ensure that our organization is fully capable and prepared for this level of growth.

III. Risk Assessment

a. Analysis of Environment

Careful analysis of the environment in which retail companies engage in operation is essential to understanding the potential for information security failures. As a retail company, the environment consists of physical locations such as brick-and-mortar outlets, online storefronts, hardware servers, point-of-sale terminals, and computer systems, as well as intangible locations and assets such as software, network infrastructure, and customer data. Prior to developing a comprehensive risk mitigation strategy, we must understand what precisely needs to be protected. In retail, among the most important types of information needing protection is consumer credit card data used in point-of-sale (POS) transactions: "cybercriminals have an insatiable thirst for credit card data. Given that large retailers may process thousands of transactions daily through their POS and there is a thriving market for stolen credit card data, it stands to reason that POS terminals are in the crosshairs of cybercriminals" (Symantek n.a.s. 2015). In this case, both the credit card numbers, and the hardware used to process transactions need to be safeguarded. In addition to credit card information, many retail companies collect other customer information to be used in data analytics: "retail data analytics is the process of collecting and analyzing data, such as customers' shopping patterns and purchase frequency, to improve operations and increase sales' (Ohio University 2020). Organizations must handle and store this data carefully and selectively, to ensure security and adhere to regulations.

An important aspect to consider is the location in which data is stored. If on site, in a server room in this example, how is that server room protected? Not only does the stored data itself need protection, but so too does the physical component of how it is stored.

To summarize the most important assets the organization must consider with regard to information assurance, we have:

Customer Data such as credit card numbers and personal information.

Physical Network Infrastructure such as POS terminals, servers, and network access components including routers, firewalls, etc.

Human Assets, the backbone of our operations and the weakest link in terms of potential data breaches: “cybercriminals are far more likely to target people within an organisation [sic] than attempt to access a network through a technological vulnerability” (Alashe 2020).

The current protocols and policies in place do not specify best practices for the securing of server infrastructure, nor the risk mitigation efforts in place in the event of environmental risk factors. Furthermore, the human factor is not properly addressed via substantial employee security training protocols.

b. Threat Environment

While the environmental analysis provides insight as to *what* types of assets need to be protected, a closer look at the threat environment lends a better understanding of what they are being protected *from*. For example. With regard to the servers where sensitive data is stored, “whether you have a small equipment closet or a large data center, the environment that surrounds your servers is critical. Servers crash. Fires damage equipment. Air conditioning systems fail. Intruders sabotage systems. Water pipes break. Employees cause accidents. The possibilities are endless and they can impact productivity, delivery, inventory, sales, staffing, and

the bottom line" (Sensphone n.a.s. 2020). We must examine and understand threats to sensitive assets from all angles.

The threats can be broken down into different realms. Physical threats can be internal, external, or human. Internal threats are things from within our organization and might include the threat of fires, power surges or outages, and issues with temperature and humidity that can damage network infrastructure. External physical threats can include natural disasters such as tornadoes, earthquakes, and floods that we have no control over, but can prepare against. Finally, human physical threats include vandalism/mistreatment of infrastructure, theft, and damage caused as a result of human error (i.e. poor network infrastructure configuration such as servers or routers). Non-physical threats, also called logical threats, are especially important in the retail industry because they can lead to data and cyber security breaches, data loss/corruption, and degraded operations due to network outages or damage. Examples of these kinds of threats include computer viruses, spyware, worms, trojans, denial of service attacks, and phishing among others.

c. Best Approaches

Now that we've analyzed the assets needing protection, and the type of threats that they face, we can take measures to implement best practices in our security protocols and procedures. The following explains the best approach mitigation tactics to be implemented against the current threat environment:

Physical: Fires can be prevented with the implementation of an automatic fire detection systems and waterless fire suppression system to safeguard network equipment. HVAC can be used to monitor and control temperature and humidity, while power issues can be addressed with the use

of voltage controllers. Lightning protection systems can be installed to route and focus high energy strikes away from critical infrastructure, and flooding can be mitigated by placing servers and other network components in physically higher locations such as upper floors rather than in basements. To address human threats, access control such as door locks and electronic password-based entry should be installed. Employee security awareness training should be implemented in all departments, with an emphasis on phishing and password best practices.

Non-Physical (logical): Anti-virus software should be used to protect against trojans, viruses, spyware, worms, etc. Intrusion detection/prevention systems should be implemented to monitor the network and protect against denial-of-service attacks. Log management and Identification and Access Management should be implemented as part of a broader network monitoring and control policy that will help establish baseline norms and defined user access privileges. Finally, as opposed to current organizational policy, stronger authentication methods must be implemented to prevent unauthorized access to computer systems. Such methods might include multi-factor authentication, password best practices (with an emphasis on training; stronger passwords), and smart cards/biometrics for access to the most sensitive server locations.

d. Risk Matrix

A risk matrix may be utilized to better understand and illustrate the threats and vulnerabilities faced by this organization. The benefit of this style of matrix is its ease of use, flexibility, and low cost: “since the assets, threats and vulnerabilities are constantly changing, an adaptive easy to use methodology is valuable to companies for conducting risk assessments internally” (Chen and Goel 2005).

When analyzing the matrix, the likelihood of a given risk occurring is on the left side, and increases from top to bottom. The severity of impact that the risk entails is located across the top of the matrix, and increases from left to right. The following examples can be found in the matrix:

Unlocked Doors (to server room)

Risk Level 3: high probability and medium severity

Examination: The probability of this risk is high due to the effects of human nature (i.e. forgetfulness/distraction) and the ease of occurrence. The severity of risk is medium, or 1 on the risk rating key, because mitigation efforts should be made. If the wrong person gains access to the server room they could infect the network with malware or cause physical damage to network infrastructure.

Mitigation: Automatic locking doors with secure keypad or badge entry should be implemented.

Natural Disaster (Earthquake)

Risk Level 5: medium probability and medium severity

Examination: The probability of this risk is medium, meaning the risk will probably occur. Due to the widespread geographic nature or our retail operations, there is likelihood of some sort of natural disaster like an earthquake occurring somewhere at some point. The severity of this risk is medium, as mitigation efforts should be made

Mitigation: Server racks and network infrastructure should be bolted down and secured from falling. Additionally, special care should be taken when choosing the location of these items as earthquakes may lead to secondary hazards such as flooding due to burst pipes.

Distributed Denial of Service Attack

Risk Level 8: medium probability, high severity

Examination: This risk is in the probable zone due to constant efforts by hackers to disrupt retail operations and inflict financial harm. The severity level is high because a successful DDoS attack can result in the online storefront being unreachable by customers, having a direct and immediate impact on sales. Furthermore, it is possible that in this event customers will look elsewhere to acquire goods, creating a potential for decreased brand loyalty and impacted future sales once the website is up and running again.

Mitigation: The utilization of firewalls to limit unwanted network traffic, intrusion detection and prevention systems to identify malicious or abnormal traffic patterns, and a unified threat management (UTM) to better understand, optimize, and protect the network.

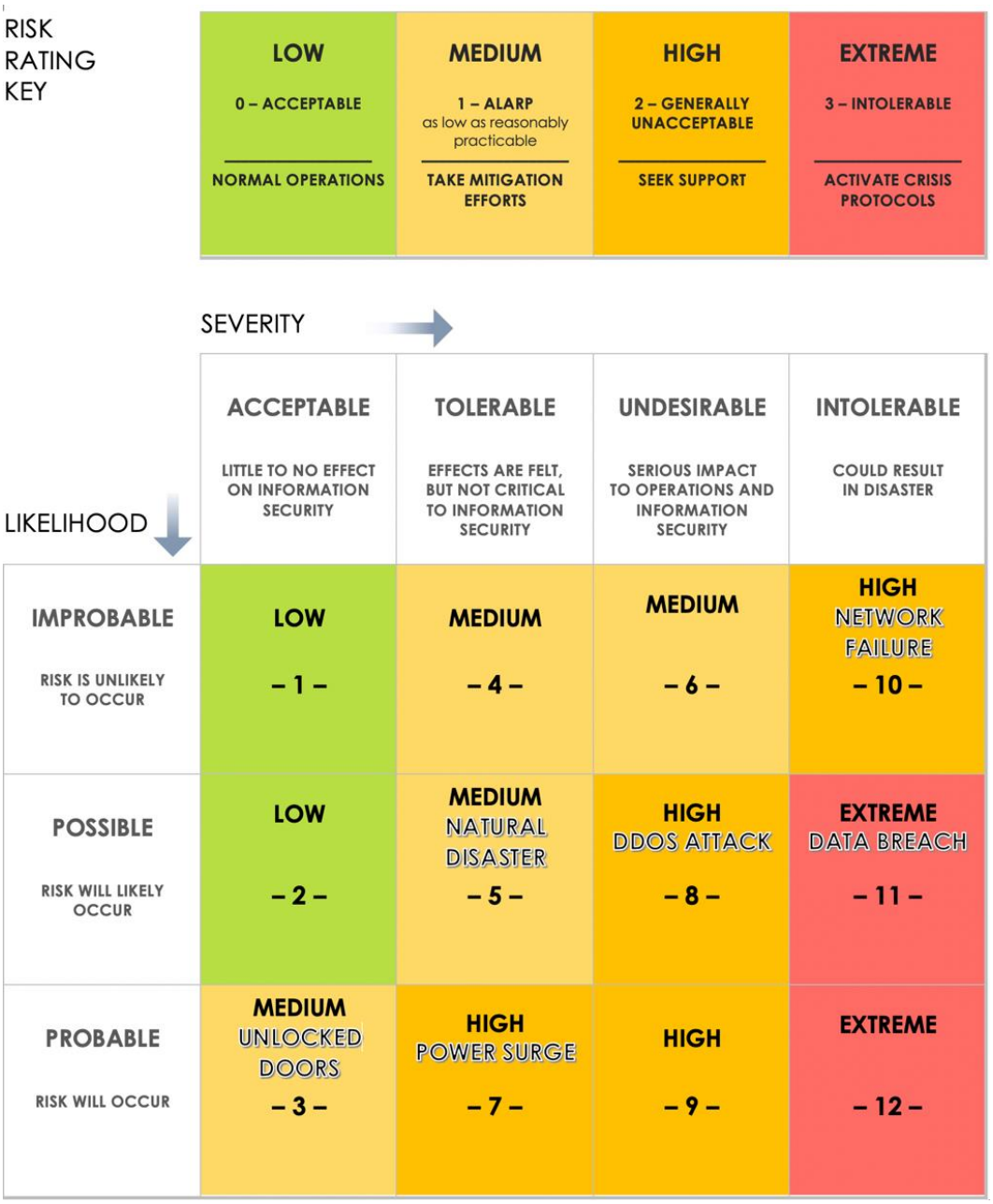
Data Breach

Risk Level 11: medium probability, extreme severity

Examination: This risk falls in the mid-level probability range due to constant efforts of hackers and nefarious actors. The severity is extreme as a result of the impact a data breach can have, including financial loss, reputational loss, lawsuits, regulatory fines, and more. Data breaches have become an increasingly common occurrence and can sideline operations and result in major organizational shifts as can be illustrated by the Target data breach that affected millions.

Mitigation: Security training needs to be implemented at every level of the organization, with an emphasis on human vulnerabilities in phishing attacks. These types of attacks have been responsible for many data breaches in which attackers gained network access by tricking

company employees into giving out their passwords. Security software should be implemented and up to date in all computer systems, from employee terminals, online storefronts, and POS devices. Regular security auditing should be implemented to ensure all systems and employees are prepared for potential attack and the resulting breach that may occur.



IV. Statements of Policy

Now that the information assurance threats and vulnerabilities have been properly identified, we can outline the appropriate protocols and mitigating factors in the form of policies and procedures. The following sections will provide a structured methodology for addressing security incidents.

A. Incident Response Protocols

For these purposes, an incident will be defined as a non-routine event that disrupts IT services, as outlined in the preceding risk matrix.

Preparation

The first step in achieving satisfactory incident response lies in the preparation. The creation of an incident response team (IRT) is critical to this effort, as this team will work together in a coordinated effort to address and mitigate the incident, as well as spearheading communications during and after. The Vice Presidents of IT and Cyber Security will both be a part of this team, as they will be responsible for directing the efforts of their appropriate teams and acting as communication liaison with upper management. This incident response team will also be in charge of performing ongoing collection and analysis of threat intelligence feeds, as well as conducting cyber hunting exercises. Another important aspect of preparation is the development and implementation of an employee security awareness training program which is to be administered on a monthly basis.

Detection and Reporting

This section can be further broken down in to four areas: monitor, detect, alert, and report. The goal here is to ascertain the cause of the breach and ensure containment. Monitoring can be done via the use of log analysis with a focus on firewall and network traffic management. Detection can occur via the use of anti-malware programs, file integrity software that detects modified files, and again the use of logs to examine users, devices, operating systems, applications, etc. Upon detection of an event, the IRT previously identified should be alerted immediately. Finally, proper documentation and reporting must occur to ensure compliance with all applicable regulations relating to any potential breach of personal protected information.

Triage and Analysis

At this step we will collect data to be used in analysis. Efforts must be made to determine any tracks left behind by an attacker, build a timeline of events, gather digital forensics to better attribute the precise cause of the security incident on an individual device level. A detailed analysis of existing logs should occur to determine the overall scope of the compromise, and an inventory of compromised systems and network devices should be taken.

Containment and Neutralization

Arguably the most critical aspect of the response protocols is the containment and neutralization of threat, and the successful completion of this step will help get operations back to normal as quickly as possible: “the strategy for containment and neutralization is based on the intelligence and indicators of compromise gathered during the analysis phase. After the system is restored and security is verified, normal operations can resume” (Bandos 2019). Once analysis is complete, the IRT should perform a coordinated shutdown of affected devices and services to

wipe and rebuild them, including a mandatory password change for all affected devices. If the incident is an external attack, all IP addresses identified as having been used by the attacker should be blocked.

Post-Incident

Finally, an incident report must be created to outline and document the occurrence. This report should identify any failures in security that can be learned from, and the development of additional protocols should be suggested if they would have inhibited the incident.

B. Justification of Incident Response Protocols

Successful incident response protocols will ensure the proper anticipation of, and reaction to, security incidents, allowing the company to continue operating with the minimal level of impact possible: "enterprise architecture and systems engineering must be based on the assumption that systems or components have either been compromised or contain undiscovered vulnerabilities that could lead to undetected compromises. Additionally, missions and business functions must continue to operate in the presence of compromise" (Zurkus 2019).

The response protocols are heavily geared toward external threat actors compromising our systems, and the use of log/network monitoring because "over the last few years (2014 to 2019), attacks have made the swing away from Point of Sale devices and controllers, and toward Web Applications. This largely follows the trend in the industry of moving transactions primarily to a more web-focused infrastructure...personal data figures prominently in Retail breaches and is more or less tied with Payment for the top data type compromised" (Verizon 2020). By

following the protocols in the event of identified security vulnerabilities (data breach, DDoS attack, Network Failure, etc.), the organization will most quickly recover operations and prevent a recurrence of the incident type: “being proactive allows organizations to better react with a deeper understanding of the threat actor’s intentions and how the organization’s defenses relate to potential threats” (Zurkus 2019).

C. Disaster Response Protocols

Disasters can manifest in many different forms, for example electrical fires, broken waterpipes, and natural disasters (tornado, earthquake, flood, geomagnetic storm, etc.). In the event of these occurrences it is appropriate to have protocols similar those in the incident response section, and a disaster may also elicit the need to enact the incident response protocols dependent on its effects on the network. The following protocols should be followed in the event of a disaster:

-Declare a disaster: this will be the responsibility of the Chief Risk Officer (CRO), who will determine whether the impact to the organization is sufficient enough for the declaration.

-CRO Contacts both CIO and CISO to enact chain of events in IT and Cybersecurity departments.

-Activate Emergency Response: this includes addressing the immediate physical threats such as extinguishing fires or removing water.

-Initiate offsite data backup to secure sensitive data in the event of further damages or secondary disaster. Fires may smolder and reignite, and earthquakes could have aftershocks causing even more damage to infrastructure.

-Assess critical applications and devices for damages and weakness.

-Commence recovery operations.

-Review event timeline to determine appropriated changes to infrastructure or security factors that would have prevented or mitigated damage from the disaster.

D. Justification of Disaster Response Protocols

Following the disaster response protocols will ensure recovery and a return to normal business operations as soon as possible, to the benefit of customers, employees, and stakeholders. These protocols ensure continuity of business and data safety by providing for safe backups and a pre-determined response that can be quickly initiated. This is important because "studies show that more than 40% of small businesses close permanently after a disaster. Among the businesses that reopen, another 25% fail within a year...a good disaster plan means fewer days out of business, better communication with customers, and a better settlement from your insurance company. Add it all up and your plan could be the reason your small business beats the odds" (Brooke 2021).

E. Access Control Protocols

Physical access controls must be implemented to secure all network devices that have access to sensitive data. Electronic locks should be installed on server rooms, and employee terminals must be behind counters. WIFI access points within brick-and-mortar retail locations must be secured using WPA2 and routers and other sensitive network equipment should be behind locked doors.

Logical controls will control who can access the network, and should be implemented using role-based access controls: “the role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks” (Lutkevich 2020). This will help safeguard sensitive data by limiting how many different employees can access it based on their work responsibilities, “access can be based on several factors, such as authority, responsibility, and job competency. In addition, access to computer resources can be limited to specific tasks such as the ability to view, create, or modify a file” (Zhang 2020).

F. Justification of Access Control Protocols

Limiting who can access resources will help keep the organization compliant with regulations such as GDPR and the CCPA, which recommend “after analyzing the personal data and their permissions, put in place the right permissions. A very effective security measure is to limit data access to those who need it as part of their job or Role-based Access Controls’ (Green 2020).

Furthermore, limiting access to sensitive equipment to designated individuals authorized to work on it, such as IT engineers, will lessen the chance of malware insertion or network tampering by insiders. The access control mechanisms employed will keep logs of who has access what within the organization, helping to identify the culprit of insider security threats and respond appropriately to strengthen protocols.

Role based access control will also contribute to operational efficiency because it “offers a streamlined approach that is logical in definition. Instead of trying to administer lower-level

access control, all the roles can be aligned with the organizational structure of the business and users can do their jobs more efficiently and autonomously" (Zhang 2020).

G. Method for Maintaining the Information Assurance Plan

The information assurance plan is to be reviewed on a monthly basis by both the VPIT and VPCS. These members will report any necessary changes in protocols to keep up with ongoing security vulnerability assessments, which should likewise be carried out monthly by their corresponding IT and Cybersecurity teams. The CRO is tasked with ensuring that this information assurance plan stays in compliance with industry regulations and should complete a quarterly review in addition to any needed updates whenever new/pertinent legislation is enacted. Overall, the maintenance plan will consist of the following five key areas:

External Monitoring: This consists of awareness of new and emerging threats and vulnerabilities. Comparison between this data and the current plan ensure any need for improvement or alteration is met.

Internal Monitoring: This can best be described as "an informed awareness of the state of all of the organization's networks, information systems, and information security defenses. This awareness is important for internal networks which interface directly with the external networks" (Fox 2021). This is especially important as a retail organization with an online presence using a network to connect inventory and logistics.

Planning and Risk Assessment: This is inclusive of the plans outlined above wherein the information assurance plan is regularly audited and tested.

Vulnerability Assessment and Remediation: This involves the use of cybersecurity teams to conduct network penetration testing, as overseen by the VP of Cyber Security.

Readiness and Review: The information assurance plan is not meant to be a static object, but rather a dynamic, evolving part of the organization. As cyber threats and other potential information security vulnerabilities continue to grow, so too should the plan. This means a constant state of readiness in response to these new threats and ongoing evaluation of their development. This accounts for the mandated, regular reviews outlined at the beginning of this section.

H. Justification of Maintenance Plan

The maintenance plan is justified because it ensures our information assurance plan will not become outdated and our organization will stay in regulatory compliance. Regular audits, testing, and training provide for ongoing improvement and information security assurance: "every organization should have an information security program, which most people recognize. However, what most *don't* realize is that their program needs proper upkeep or maintenance. There should never be a point where an organization is overconfident after implementing a security program because there is always room for improvement" (Fox 2021).

Upon implementation, the plan will help the organization continue operations uninterrupted, and protect sensitive company and customer data from nefarious actors. In doing so, the reputation of the company will be maintained at a high level within the retail industry, as well as amongst the general public. These policies and procedures set a high standard, by which we will continue to adhere, pioneering a new level of information security within the retail industry.

V. Conclusion

a. Summary of Need for Information Assurance Plan

The need for a comprehensive information assurance plan (IAP) for this company goes beyond simple data protection. Having this plan in place and correctly followed serves the very longevity of the organization by ensuring key stakeholders have their needs met, and various legal and ethical responsibilities are maintained.

Legal responsibilities covered in the IAP are highlighted by its adherence to regulations such as the GDPR and CCPA. The risk matrix in section III of the plan, as well as incident response protocols in section IV, help meet regulatory obligations such as Article 32, section 2 of the GPRP which states "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational [*sic*] measures to ensure a level of security appropriate to the risk" (GDPR 2021).

Ethical Responsibilities arise out of the trust our customers place in us as an organization. It is imperative, especially with the ongoing growth in online retail sales, that customer information is kept safe and secure from various threats. This plan addresses how to deal with hacking, data breaches, and current security shortfalls, thereby meeting this ethical obligation to our customers. The extreme importance of this responsibility cannot be overstated, as without customers a retail company cannot continue to exist.

Without this plan in place, valuable time and resources will be wasted attempting to determine the appropriate reaction to critical situations. In the event of a system outage or data breach, time is of the essence, and every moment offline results in loss of revenue and reputational damage. Having a clear and concise method of reaction and mitigation will avoid this and ensure the company is well prepared to overcome any information assurance incident. This strengthens the company as an entity, arming it with preparedness that could potentially be the difference between recovery, or total operational failure.

b. Defense of Key Elements of Information Assurance Plan

The overall success of this IAP is contingent upon the successful implementation of its key elements, and a clear description as to who within the organization is responsible for meeting them. The ability for multiple roles, teams, and departments to meet their obligations outlined within the plan will ultimately result in a cohesive, unified approach to information security. Key elements of the plan are as follows:

Defense of Data

Data is the lifeblood of our operations as it is key to processing purchases, managing customer loyalty programs, and supply/logistics. Keeping this data safe and protected is vital to the interests of the company and this responsibility falls on several members. It takes the concerted efforts of the IT department, Cyber Security department, retail employees, and management to identify when and where efforts to follow the IAP are not being met. The C-level management team must provide the funding and tools for departments to adequately meet their individual roles and responsibilities as they pertain to data interaction.

Regulatory Compliance

Ongoing regulation has made protecting consumer data an absolute requirement. The Chief Risk Officer (CRO) is tasked with keeping abreast of new regulation and ensuring each department within the company is meeting developing standards. The precise way (technicalities) in which these standards are to be met will be determined by the CISO and CIO, and ground level application will be implemented by the VPs of IT and Cyber Security alongside their teams.

Ethical and Legal Considerations

In retail, customer sales are the lifeblood of profitability. With the vast majority of sales incurred using electronic methods, our organization has a legal and ethical responsibility to safeguard this the data processed. This is an area of growing importance, with studies showing "80% [of people] prefer cards over cash...[and] 41% of credit card users have retail and store-specific credit cards—the most common types of credit cards" (Shepherd 2020). Not only do retail employees such as cashiers have a responsibility to safeguard card numbers during transactions, but so too should IT and Cyber Security employees do their part to best protect data and adhere to the law, with their department heads being notified immediately of any breach in protocol.

Incident/Disaster Response Protocols

In the midst of a high stress security incident, there can be a tendency for emotion to run high and panic to set in. That is not the time to consider ways in which to prevent interruptions in network services or operations, or consider what next steps to take. These things should be pre-planned and rehearsed, as outlined in the IAP. Doing so creates a competent, prepared workforce that has the tools and procedures at hand in the event of emergency. In such an event,

management should be immediately notified, and the severity (as judged in the preceding risk matrix) should determine how high up the chain of command initial notification goes. For cyber security or network device compromise, the VPs of those departments must be notified immediately to begin direction of countermeasures and mitigations via their corresponding teams.

Access Management

The fewest people interacting with sensitive data or network locations creates the least amount of possibility for things to go wrong, intentionally or inadvertently. From the lowest levels of the organization, we must have a "see something, say something" posture. For example, if a cashier notices a coworker forget to lock their workstation, or leaves a door propped open that should be locked, this should be brought to their attention, as well as to the attention of next level management to be reviewed in the monthly employee security training. Creating this level of attention to access management serves to protect customer data and keep the organization in line with current laws and regulations. The precise methods and policies to be included are to be directed by the CRO and implemented by lower management.

Employee Security Training

Perhaps among the most vital key component of the IAP is an intentional pivot toward security training and education at every level across the company. The human factor is often exploited when it comes to information security, especially with the increasing amount of phishing and malware attacks against enterprise networks. Instituting ongoing training, as designed by the CIO and CISO and implemented by the Human Resources department, will greatly strengthen

security of the entire organization, helping to drive home the necessity and importance of this plan.

In conclusion, the adoption of and adherence to this IAP is a logical, cost-effective, and justified measure. It serves the organization as a whole, as well as all constituents involved in the ongoing successful and profitable retail operations. The plan provides strength of security in an informed manner, leaving our company better protected and prepared for any information assurance eventuality. The depth of reasoning and protocols outlined will not only offer protection, but very well may lead to great competitive advantage within our industry.

References

Alashe, Oz. 2020. Silicon Republic. Major Data Breaches Are Far Too Common, With Human Error Often Being a Cause. https://www.siliconrepublic.com/companies/oz-alashe-cybsafe-data-breaches

Bandos, Tim. 2019. Digital Guardian. The Five Steps of Incident Response. https://digitalguardian.com/blog/five-steps-incident-response

Chai, Wesley. 2021. TechTarget. Confidentiality, Integrity, and Availability (CIA Triad). https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Chen, Vicki, and Goel, Sanjay. University at Albany School of Business. Information Security Risk Analysis- A Matrix-Based Approach. https://www.albany.edu/~goel/publications/goelchen2005.pdf

CIO Source. 2018. What is the Difference Between a CIO and a Chief Information Security Officer? https://www.ciosrc.com/blog/what-is-the-difference-between-a-cio-and-a-chief-information-security-officer/

Cloudian. 2021. Data Protection. Data Availability: Ensuring the Continued Funtioning of Business Operations. https://cloudian.com/guides/data-protection/data-availability/

Costa, Claire D. 2019. Medium Article. The Importance of Information Security For Your Business. https://medium.com/@harish_6956/the-importance-of-information-security-for-your-business-9a0fe0bb1e34

Cranor, Lorrie. Federal Trade Commission Blog. Time to Rethink Mandatory Password Changes. https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

Edelman, Gilad. 2020. Wired Magazine. California's Privacy Law Goes Into Effect Today. Now What? https://www.wired.com/story/ccpa-guide-california-privacy-law-takes-effect/

Feliu, Carlota. 2021. Databerg Blog. Why is Data Integrity Vital for Retail Companies? https://blog.datumize.com/why-is-data-integrity-vital-for-retail-companies

Finjan. 2017. Finjan Blog. What is Non-Repudiation? A Closer Look at the Principles, Techniques, and Best Practices. https://blog.finjan.com/what-is-non-repudiation/

Fox, Thomas. 2021. Tech Experts. Does Your Security Program Need Maintenance? https://mytechexperts.com/does-your-security-program-need-maintenance/

General Data Protection Regulation (GDPR). 2021. Complete Guide to GDPR Compliance. https://gdpr.eu/article-32-security-of-processing/

Green, Andy. 2020. Varonis Blog. Compliance and Regulation. California Consumer Privacy Act (CCPA) Compliance Guide. https://www.varonis.com/blog/california-consumer-privacy-act-ccpa/

Korolov, Maria. 2020. CSO Feature. 9 CCPA Questions Every CISO Should Be Prepared to Answer. https://www.csoonline.com/article/3518436/9-ccpa-questions-every-ciso-should-be-prepared-to-answer.html

Kumar, Nitish. Webkul Blog. The Future of eCommerce in 2021. https://webkul.com/blog/future-of-ecommerce-in-2021/

Lutkevich, Ben. 2020. Tech Target. Access Management, Access Control. https://searchsecurity.techtarget.com/definition/access-control

Marks, Shayna. 2014. Business.com. What Target Should Have Done to Prevent Their Security Breach. https://www.business.com/articles/target-done-prevent-security-breach/

Ohio University. 2020. Business Analytics Blog. How Major Retailers Use Retail Data Analytics to Target Shoppers. https://onlinemasters.ohio.edu/blog/retail-data-analytics/

Samuels, Mark. 2020. ZDNet. Under Half of CISOs Are Ready to Respond to a Cyberattack. https://www.zdnet.com/article/what-is-a-ciso-everything-you-need-to-know-about-the-chief-information-security-officer/

Shepherd, Maddie. 2020. Fundera Spending Statistics. 19 Cash Vs. Credit Card Statistics. https://www.fundera.com/resources/cash-vs-credit-card-spending-statistics

Sensaphone, no author stated. 2020. 6 Environmental Threats to Data Centers and Computer Rooms. https://www.sensaphone.com/files/Data_Center_Flip_Book/mobile/index.html#p=1

Symantec, no author stated. 2015. Symantec White Paper. Cyber Security For Retail Services. Strategies that Empower your Business, Drive Innovation and Build Customer Trust. https://docs.broadcom.com/doc/cybersecurity-retail-en

Verizon Data breach Investigations Report. 2020. Retail Industry Analysis. https://enterprise.verizon.com/en-gb/resources/reports/dbir/2020/data-breach-statistics-by-industry/retail-data-breaches-security/

Zhang, Ellen. 2020. Digital Guardian. Data Protection 101: What is Role Based Access Control: Examples, Benefits, and More. https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more

Zurkus, Kacy. 2019. The Edge. Why Every Organization Needs an Incident Response Plan. https://www.darkreading.com/edge/theedge/why-every-organization-needs-an-incident-response-plan/b/d-id/1335395