A report prepared in partial completion of
The CYBR 7930 Capstone course

Security Operations Program Design

Wessly Soronellas

November 21 2021

Contents

Executive Summary

The purpose of this document is to address the concerns of management regarding the potential limitations the company may face during geographical expansion. The current security operations are adequate given the current business model; however, should the organization continue to expand across the United States, there are legitimate concerns that must be addressed to ensure business operations can continue whilst also maintaining information security.

The document contains the current security structure implemented by the organization as well as a proposed security design labeled as intended security operations. Additional sections including a deployment strategy of the proposed design as well as a Security Run Book template to assist in implementing or modifying security services. The report concludes by discussing the potential factors executives must make when deciding on a course of action as well as the recommendations resulting from the report.

Problem Statement

There is a consensus among businesses that departments like Information Technology (IT) and Information Technology Security (ITS) are viewed as cost centers to an organization. While this statement is true in regards of what services these departments provide for the organization are necessary for its operation, the goal is to better isolate these departments from other departments except when necessary.

The best way for DHHI to operate effectively and efficiently is to allow each department to perform its intended business functional with limited interruption. This is accomplished by creating a security structure which limits inter-departmental dependency by creating a secure configuration that does not rely on the user to assist in ensuring information is secured appropriately.

This configuration can best be viewed as a holistic ecosystem of separate departments that perform functions individually in a self-sufficient manner that reduces reliance on other departments. While the organization strives for an open-door policy encouraging open communication, it also understands that efficiency is best accomplished by limiting inter-departmental interaction. An example of a successful implementation of this security model would allow the sales team to access its necessary resources while limiting its responsibility in ensuring security like reporting fraudulent emails, ensuring systems are configured with the most recent software versions, ensuring information is traveling via a communication channel compliant with the organization's encryption policy. Should this design be implemented, the goal is to reduce the time and effort currently being utilized by outside departments in ensuring system information is complying with company policies.

Scope

This security design is intended to apply to all employees at DHHI; however, to better prepare the organization to grow with minimal barriers, the goal of this security design is to become more efficient in how employees spend their time at work. Therefore, the design was created with the intention of having each department focus as much time as possible performing relevant functional duties rather than operational procedures related to Information Security. The result of this strategy is a reduction in the number of operational procedures identified in the Omnibus that rely on employee initiation coming from other departments not related to Information Security or Information Technology.

Current Security Operations

Security Services

Currently, Diamond Hands Holdings Inc. (DHHI) has an environment which utilizes security controls effectively in terms of providing adequate security to all information and information systems used by the organization. While there are areas in the design that could be modified to better increase efficiency, the overall security posture of the organization is sufficient. All security services currently being utilized by DHHI are mentioned in the following sections. Each section will include, when applicable, a brief description of the current service, any policies or procedures accompanying the service, and any planning regarding implementation, deployment, training, etc.

Vulnerability Management

The Azure Monitoring Service is used as a monitoring service for cloud services to identify any vulnerabilities within any of the hosted virtual machines. Change management such as version management is in accordance with the specified policy stating update management in the organization's Omnibus.

Threat Detection & Threat Intelligence

Microsoft's Protection Office is used to conduct investigations on email communications as well as to monitor and, if possible, prevent security incidents from occurring. Policies containing acceptable use are outlined in the Company's Omnibus. This service is owned and operated by the Cyber Triage and Forensics (CTF) team.

Detection Engineering

Carbon Black is the security service used for triage and forensics during investigations classified as a potential security incident. This service as well as all processes are owned and operated by the CTF team; therefore, all updates to systems and processes must be approved by the CTF Director.

Incident Response

Splunk is currently being utilized as the SIEM that is used for reporting, triage, and incident response. This security service includes Archer RSA which is used to provide the Information Security subcommittee their requested reports. All IDS signatures and software versions will be updated every two weeks if available with data being retained for at least a year. The CISO owns this product and its accompanying processes; therefore, any changes to any components dealing with this service must be approved by the CISO.

Access Control & Provisioning

Active Directory, Active Directory Service, and the HRIS are of the information systems used by DHHI in implementing access control and provisioning. While these services are technical controls used to enforce confidentiality, policies and procedures identified in the Omnibus provide additional detail outlining the roles and responsibilities of employees.

Application Security

Agari provides application security regarding email communication. Anti-malware software is required on all DHHI systems as specified in the Omnibus as well as guidelines outlining acceptable use on various applications.

Disaster Recovery

Disaster Recovery is outlined in the Omnibus which outlines the roles and responsibilities of individuals should a disaster occur. Additionally, the plan states what elements should be prioritized in the event of a disaster as well as the time frame allowed for the recovery to take place (14 days). This plan is tested bi-annually with annual reviews performed by necessary personnel.

Intended Security Operations

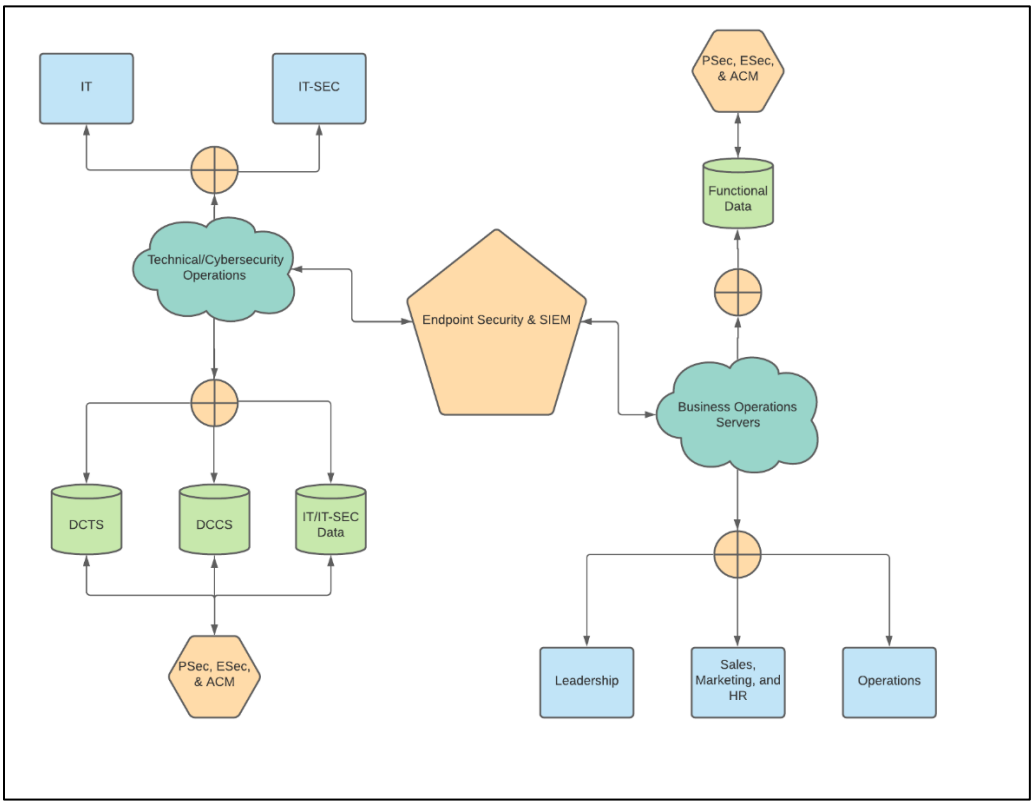

Figure 1. Intended Security Operations Function Diagram. This figure displays how each department should function within the intended security operations design.

Security Services

As the organization continues to grow and expand across the nation as well as possibly reaching global markets, DHHI must continue to enhance its security posture to ensure its information and services are adequately protected; therefore, the security services stated in this section aim to not only secure the company at its current state, but also provide a foundation which allows DHHI to expand its services without sacrificing its security posture (please refer to *Figure 1* for a diagram of how the design would look if implemented).

Each section will identify the security service and its intended function as well as a justification why that service is selected. It's important to identify why each service should be implemented to better understand its importance in the overall design. After all security services are identified, a budget containing the costs and cost recovery will present the estimated costs of implementing each security service listed.

Risk Management - RM

Risk Management will manage cybersecurity risks and verify that the company is compliant with internal policies and standards for implementing risk management. Organizational policies, standards, and procedures should be regularly reviewed and updated, as necessary based on an ever-changing threat landscape and updates to National, State, and local laws and policies.

IT Security Architecture - ITSA

This service will entail strategic planning and development of a DHHI IT infrastructure that supports the mission and the security objectives. Development of an enterprise security architecture diagram. This will require identifying its business needs, functional requirements, security requirements, and risk assessments, as well as the security controls in place. The IT security architecture should be annually reviewed to ensure that the business needs are met and that the security posture has not been degraded.

Penetration Testing / Security Assessments - PTSA

All assessments included in this service involve performing testing and security assessments of DHHI information systems, applications, and networks. Such testing will involve network and application penetration testing. This can be performed internally or outsourced to a service provider. Penetration testing is necessary to ensure that network and other IT resources' vulnerabilities are identified so that they can be remediated. This will reduce the likelihood of the organization succumbing to cyber-attacks.

Training & Awareness – T&A

Training and Awareness will provide role-based training for DHHI IT personnel and awareness and education for all employees DHHI. Securing DHHI Information systems and data cannot be achieved without skilled, knowledgeable, and trained personnel at all levels.

Access Control Management - ACM

As a security service, Access Control Management will manage access to IT resources at DHHI, to include performing account reviews, approvals, authorizations, and modifications that account for position changes, promotions, and terminations. Access to the organization's IT resources must be restricted by the principle of least privilege to reduce the likelihood of unauthorized access or disclosure of sensitive information.

Cloud Monitoring & Storage – CM&S

This security service will provide online backup and documentation storage. Documentation stored on the local file servers should be backed up to the cloud to ensure continuous operations in the event of a disaster.

Vulnerability & Patch Management - VPM

Vulnerability and Patch Management will develop a process to manage vulnerabilities in information systems and apply patches to systems in timely manner. Will require investment in a vulnerability scanning tool. Vulnerability & patch management will enable DHHI to adequately identify weakness in information systems and remediate in a timely manner before exploitation of those vulnerabilities.

Vendor Risk Management - VRM

This service will perform risk assessments against new suppliers to verify that they meet the minimum-security standards to process data from DHHI. Additionally, employees must document the status of the risk assessments and track any findings for monitoring and auditing purposes. The supply chain can be a risk to DHHI because the products they provide could be counterfeit or contain malware, which could cause disruptions at DHHI and could potentially lead to data breaches (Boyens, Paulsen, Moorthy, & Bartol, 2015).

Security Information & Event Management - SIEM

The SIEM will log correlation and alerting from various systems such as firewall, IDS, IPS, servers, etc. This helps the security operation team to better correlate incidents and respond to alerts in a timely manner.

Environmental Security - ESec

Environmental security will outfit the server room with fire resilience and drainage equipment to protect IT resources in the case of an emergency and maintain the equipment. The server room must have the proper fire protective and drainage equipment installed to prevent damage to any IT resources in the event of a casualty. It is also necessary to regularly test the equipment to make sure that it operates correctly.

Physical Security - PSec

To implement this security service DHHI must install and maintain proximity readers to restrict access to the server room. Access to the server room should be restricted to only those who require access as part of their duties. Maintaining the proximity readers will ensure that only the properly badged personnel can enter the space.

Incident Response - IR

DHHI will execute incident response measures for all cyber security incidents. It is essential for a business to have a dedicated team of individuals that can detect, contain, eradicate, and recover from an incident (Cichonski, 2012). This will ensure that any successful cyber-attacks, spillage events, etc. are responded to efficiently to minimize damage and restore operations quickly

Disaster Recovery - DR

The Disaster Recovery Plan identified in the current security operations section is sufficient and will therefore continue to be plan utilized by the organization. No changes on this section are necessary.

Data Center Technical Services - DCTS

These are the services that are technical services used for general purposes including user management, networking, storage, etc. Within this security service, the following servers along with their main function are identified as: server I - Dell Storage NAS #1, server P - Dell Storage NAS #2, server T - Active Directory Service, server X - Dell Storage NAS #3. These services are necessary for critical business functions such as file sharing and access management and are therefore necessary to ensure the organization can continue operations without interruptions. Additionally, this service provides DHHI the capability to perform backups, which is essential for contingency planning purposes (Swanson et al., 2010).

Data Center Cybersecurity Services - DCCS

These are the services that are explicitly information security related. Within this security service, the following servers along with their main function are identified as: server J - Active Directory, server K - SPLUNK, server L - Carbon Black, server M - Agari, server O - AZURE Monitoring Service. As a company specializing in Governance Risk and Compliance and Information Security consulting services, it is necessary to perform these services to maintain reputation as a leader in the security field as well as instilling confidence with current and future customers by showcasing the organization's security posture as a reference model/case study.

Network Administration - NA

Manage network services for the organization. DHHI should implement 24/7 network operations center by the start of the next fiscal year. Administering the network includes managing the performance of the network, troubleshooting faults, and network device management. These functions will ensure that the network works as intended for normal business operations.

Cyber Risk Report Tool - CRR

This tool generates reports for security metrics, including open vulnerabilities with patch dates, number of spam emails blocked, cyber risk assessment results, etc. The effort utilized in generating these reports is necessary to evaluate ongoing security levels inside the organization and to inform those statuses with the Board of Directors to inform shareholders if necessary as well as act accordingly if action is necessary.

Intelligence Gathering - IG

Intelligence Gathering will identify any relevant cybersecurity threats and threat actors. It is critical that the organization know what cyber threats there are that could impact the business and disrupt operations with the business or its supply chain. Knowing what threats there are will help the business make better risk management decisions to mitigate the risk associated with the applicable threats.

Endpoint Security Suite - EndSec

This service will deploy and maintain endpoint protection suite consisting of anti-malware, anti-ransomware, and web protection services. Endpoint protection will reduce the likelihood that the organization is victim to malware, including ransomware, worms, etc.

Budget

While the individual security services that are listed above are important in identifying specific areas each service will cover, an additional measurement used in selecting appropriate services is identifying the costs associated with each service. Therefore, each security service identified in the previous sections will be included in the table below representing the estimated costs as well as the cost recovery strategy. Please note the table is meant to be a preliminary budget that contains estimated costs; therefore, each service may represent a different cost once implemented.

Service Name	***Cost***	***Cost Recovery***
RM	<Cost of hiring additional resource to perform these risk assessments>. <Cost per DHHI employee supporting the effort, annually>.	Bill to overhead.
ITSA	<Cost to perform the strategic planning and development>.	Bill to overhead.
PTSA	<Cost per employee performing the test> <Cost of outsourcing the tests, if necessary>.	Bill to IT Security.
T&A	<Cost of purchase a security awareness tool>. <Cost of developing training and certifications>.	Bill to HR.
ACM	<Cost of the IAM tool> <Cost per employee to manage access>.	Bill to overhead.
CM&S	<Varied cost based on required storage per month>.	Bill to HR.
VPM	<Cost of purchasing a vulnerability scanning tool and hiring additional resources for remediation.>	Bill to IT Security.
VRM	<Cost is the sum of total time of assessment duration performed by employees multiplied by number of assessments in a year.>	Bill to overhead.

SIEM	<Cost of purchase a SIEM tool and implementation.>	Bill to IT.
ESec	<Cost for the equipment>. <Cost per employee maintaining the equipment>.	Bill to overhead.
PSec	<Initial cost for equipment, then any replacements due to obsolescence> <Cost per employee maintaining the equipment>.	Bill to overhead.
IR	. <Cost per employee supporting incident response team>.	Bill to HR.
DR	<Current cost of operation.>	<Current cost recovery strategy.>
DCTS	<Active Directory Services are billed per user. NAS storage servers' costs are calculated by adding the hardware costs (server, storage drives, cables, cooling systems, etc.) to the software costs (OS, BARS, etc.). The total expenditure cost should be represented as an annual amount.>.	Bill to overhead.
DCCS	<Cost to procure, implement, and maintain hardware and software> <Cost per employee administering the machines>.	Bill to overhead.
NA	<Cost per employee designated as network administrator>.	Bill to overhead.
CRR	<Cost per employee utilizing the tool and consolidating reports>.	Bill to HR.
IG	<Cost per employee supporting cyber intelligence>.	Bill to HR.
EndSec	<Initial deployment and annual licensing cost>.	Bill to overhead.

Improvement Program

Deployment Strategy

To reduce friction during implementation as well as to ensure efficient utilization of security services, a deployment strategy must be able to provide a clear and concise plan on implementation. For this reason, the improvement program includes a deployment strategy which identifies a generic guideline on how each service should be implemented, how the audience should be trained on that service, and how each service should be reviewed and updated. While each security service may contain specific details not mentioned in this section, this program should still be used as a general reference guideline.

Implementation

All security services must go through the six phases of the IT security life cycle outlined in NIST SP 800-35. (p 2, Grance et al., 2003) In addition to this system life cycle, each security service should have specified owner(s) for the system(s), data, and process(es) as well as a document identifying the roles and responsibilities of all necessary individuals in the process. This document must be agreed by management of all appropriate departments mentioned.

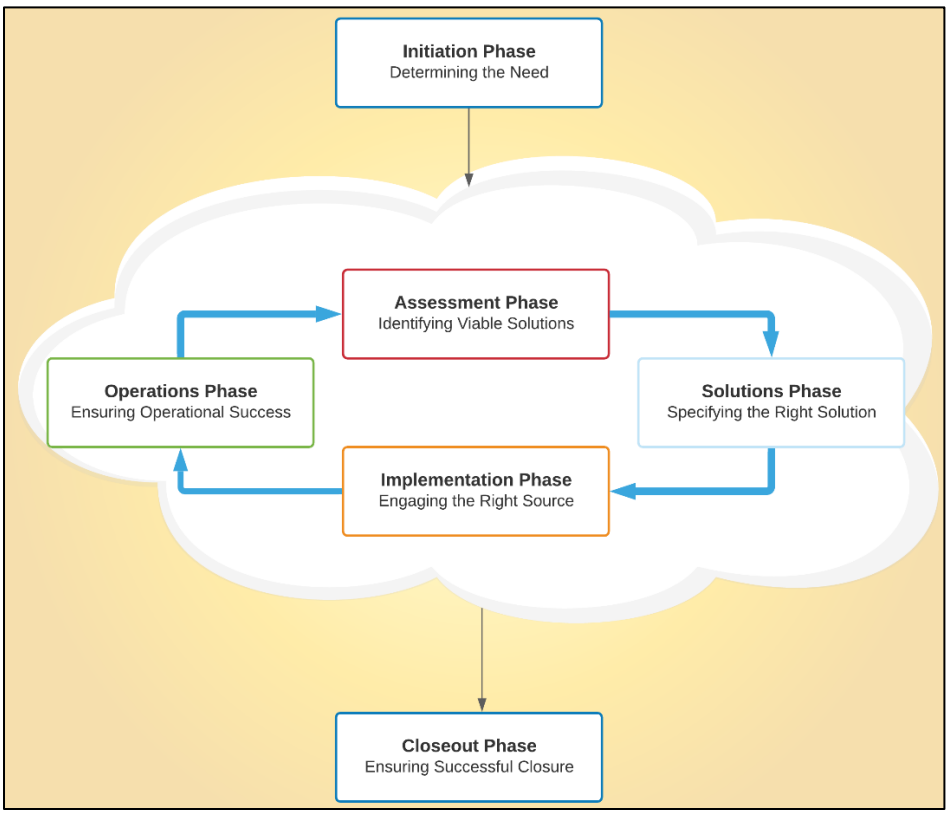

Figure 2. IT Security Services Life Cycle. This figure diagrams the life cycle of security services as mentioned in NIST SP 800-35, section 4.1.

Training Plan

Before functional users are granted access to the security service and its included components, a foundational training must be performed which provides a basis on the main function of the service and how it operates. Once the foundational course is completed, basic access is granted which allows the employee to only perform the basic, fundamental operations needed within the service. Once the employee has had enough experience with the system, an additional assessment will be performed to determine whether additional training is necessary. If the assessment results come back satisfactory, the functional user may then be granted full access as specified by management. Assessments and training may vary from service to service.

Version Management

All security services will require a review plan upon implementation which specifies the interval between reviews as well as the members involved in the review. Any changes to a security service s8uch as changes to policy, system owners, roles and responsibilities, etc. must be approved by the review committee. Any changes that must take place immediately can be done so with the approval of the C-suite member of that department which will provide a justification for the change later.

Master Security Run Book

Introduction

This run book is meant to be a general guideline used when attempting to update any elements included in the security design. Each individual update or run will include details specific to that service, yet each process aligns to the outlined process to some extent; therefore, this run book should be used as reference by management and systems analysts to ensure a security service is updated appropriately. For specific questions involving a security service, please contact the system owner.

Monitoring

In this section, mention the measurements used to monitor activity with the security services(es). Identify the threshold that exist to decide whether a security service is performing satisfactory or not satisfactorily. By labeling the thresholds or any data points that can be used to measure effectiveness, the assessment stage can be performed with limited additional effort.

Assessment

Once the measurements have been identified, decide on a time interval that will be used to collect the measurements within. This time frame should be long enough to accurately gauge a pattern of behavior in the security service. Identify all available courses of action that can be taken to improve the security service in question.

Implementation

After the assessment, review the available courses of action with decisionmakers and decide on what the next step should be in the process. This decision may be an action that calls for no action; therefore, the decision that is decided on should be noted regardless of what the action entails. Involve any individuals necessary to move forward with implementation.

Support

Once the initial implementation is completed, continue to monitor the status of the security service that was created or updated. Ensure that functional users are aware of the changes being made and have been trained on any new information resulting from the implementation. The goal in this section of the run book is to prevent friction being a barrier to employees utilizing the new functionality. Decide on an appropriate time interval to which the support can be completed. This time interval is only temporary as to reduce the friction that appears when introducing new systems and processes to departments.

Closeout

After the support period closes, perform an after-action report which identifies all the information related to modifying the security service in question. Be sure to mention any obstacles or limitations the team faced during implementation as well as suggestions to prevent future occurrences. AS the project closes out, be sure to provide the system owner with all the necessary resources to remain self-sufficient after the process is officially over.

Discussion

In reviewing this security design, it's essential to view the material as a guidance towards an idea that might never be completely resolved. Unfortunately, unexpected events may render this entire design useless; therefore, all content should be weighed given the status of the organization. Though specific suggestions were made in the previous sections, such suggestions can be taken as abstract ideas that merely advise a change relating to the topic discussed. However, should the organization continue to operate under the same structure as it was when developing this document, the suggestions made in this document were done so with the intention to provide the best security posture whilst also ensuring the company had the capability to expand if desired.

Conclusion

In conclusion, while the current security design at DHHI is sufficient to withstand current business operations, an expansion across the nation might bring about significant obstacles in continuing security operations as they are; therefore, an updated security design was created to better withstand any potential expansions to the organizations. The goal with the proposed security design is to allow each department to perform their business function with limited interruption from other departments. Only necessary security services were included in the intended security operations section to minimize expenditures; however, modifications to the design are not only welcomed but expected. Changes will more than likely need to be made to accommodate external factors, yet the design was created for the sole purpose of increasing security resiliency without limiting the ability to expand business operations.

References

Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2015). Supply chain risk management practices for Federal information systems and organizations. NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Bulim, J. (n.d). Diamond Hands Holdings Inc: Case Study (DHHI Version 2.2). Diamond Hands Holdings Inc. https://kennesawedu.sharepoint.com/:b:/s/Team-Team-CYBR7930forFall2021/Eal4er0l6ABAlNX4Vj5eXHUBVjwvLzxFAw2M0BvOXYEUq Q?e=42Hs3b

Bulim, J. (n.d). Diamond Hands Holdings Inc: Policy and Planning Omnibus. Diamond Hands Holdings Inc. https://kennesawedu.sharepoint.com/:b:/s/Team-Team-CYBR7930forFall2021/EXLSdgjsJpZPqBT_Gv0Ui6gBIM46Qh8HPJgZgwvSgxusnA?e =a5kosx

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. NIST. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800- 61r2.pdf

Grance, T., Hash, J., Stevens, M., O'Neal, K., & Bartol, N. (2003). Guide to information technology security services. NIST. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-35.pdf

Swanson, M., Bowen, P., Phillips, A., Gallup, D., & Lynes, D. (2010). Contingency planning guide for Federal information systems. NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf