MEMORANDUM

TO: EVAN BATTAGLIA, CISO, DIAMOND HANDS HOLDINGS INC.

FROM: WESSLY SORONELLAS

SUBJECT: SECURITY SERVICES DIRECTORY

DATE: OCTOBER 21, 2021

This memorandum was written for the explicit purpose of identifying all elements necessary to create and implement a security services plan for Diamond Hands Holding Inc. This plan was created for the intended purpose of identifying all security services performed in the organization as well as documenting the information about each of the services. By identifying the security services utilized within the organization, there will be a tangible document that can be used as a reference for upper management when making strategic or executive decisions on current or future security services. As discussed in the security services plan, the information included for each security service was done so with the intention of providing only the most critical information necessary for decision making (cost, value, constituency ,etc.). While the document will need to be updated as modifications are made, much of the information is presented at a high level and therefore can be applicable despite being an earlier version.

Included within this version of the security services directory (version 1.0) is an initial plan developed that documents the strategy used to create the plan. Within the plan is an explanation of important information used to implement the services table which is the main reference point in the plan that will most likely be updated the most frequent. Following the security services directory table is a summary that documented the approach taken to create the directory. The summary includes steps taken to create a complete list, a section discussing limitations during the process, as well as next steps in validating the process with relevant business units. If there is any information that appears to be incorrect, please reach out so further discussion can take place.

Sincerely,

Wessly Soronellas

Cybersecurity Process Consultant
wsoronel@students.kennesaw.edu
678-245-9654 (Ext. 5443)

Security Services Directory Plan

Purpose

The security services directory that is discussed in this section is expected to serve the purpose of providing a tangible list of security services performed by the organization. As services are identified and information is documented on each service, the goal is to provide managers and leadership a reference of the current state of the security services used by the business. By providing a services directory to decision makers, strategic decisions (adding/removing services, hiring additional staff, efficient utilization of services, etc.) can be made with more confidence, given the information available.

Plan

In deciding what information will be documented for each service, only the most important details are provided in the table. Of the possible pieces of information available to each service, the most important data points for each service were decided with the following data points: the cost (labeled as expenditure) to utilize the service; the manner to which the cost is to be recovered by the organization, labeled cost recovery; constituency, defined as which personnel are affected by the security service; the frequency or time between each service run, labeled as frequency. In addition to these data points will be a detailed description of each service (labeled description) as well as a justification (labeled justification) for why that service is necessary for business operations.

To be as inclusive as possible, the criteria necessary to qualify a service as being labeled a security service is defined as any service that performs some action related to the Confidentiality, Integrity, and Availability (CIA) triad. The action performed can range from technical controls such as firewalls to management controls such as policies related to the CIA triad.

All information collected will be done so by researching the Diamond Hands Holdings Inc. (DHHI) business plan as well as the DHHI's policy and planning omnibus to identify any items qualifying as a security service.

Plan Validation

Because some of the services listed may be identified as a security service incorrectly, all services will be validated with various members of the business unit which operates or owns the service; therefore, each entry in the security services directory can have a high degree of confidence in belonging to the directory.

Service Justification

Each service must include a justification as to how that service aligns with the company mission and why the service should remain operational. For each justification, a cost/benefit analysis should be performed to identify the net benefits the service provides to the company. Should a service lack the necessary net benefits to continue operations, the service will be included in the directory until management decides to discontinue service. The security services directory is a living document and must be updated continuously to reflect the changes made within the organization.

Security Services Directory

Service	Description	Constituency	Frequency	Justification	Expenditure	Cost Recovery
Data Center - Technical Information Security Services	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	All DHHI business-units	24/7/365	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.	<All hardware and software costs in maintaining servers online and available must be included in this section. This includes the server itself, the applications running on those servers, and the man hours required to keep those systems online. Therefore, all operations costs involved in maintaining availability must be included. This can be done by multiplying the average amount of work hours performed on each system by the pay rate of each employee responsible for servicing each system. This amount should be calculated to represent an annual expense.>	All costs will be billed to CISO and IS department
Data Center - General Technical Services	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.	All DHHI business-units	24/7/365	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.	<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.>	All costs will be billed to CTO and IT department
Board of Directors Information Security Subcommittee Reports	Reports the following security metrics to Board of Directors: detected intrusion attempts, number of spam emails blocked, vulnerability patch response times, and unpatched vulnerabilities, number of users categorized by application/data access levels, overall volume of data which CTS generates, Incident Rates/severity levels/response times and time to remediation, vendor risk management, qualitative measures of risk, and comparison with industry pers/competition.	All DHHI business-units	Reports delivered as requested by Information Security Subcommittee	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.	<calculate the total number of members involved in generating the reports and calculate the hourly pay rate for each member (even if compensation is salary-based). Identify how long it takes (in hours) to completely generate the reports and distribute them to Information Security Subcommittee. For each member, multiply hourly rate * total time to complete>	All charges resulting from generating, handling, and customizing reports are charged to the budget allocated to Board of Directors' budget.

Server Containment System	These are the services utilized to secure the physical risks to the organization's servers. These services include 24/7 monitoring via video surveillance and armed security, a climate control system with ventilation to protect hardware, and a Fire Resilient System (FRS) with drainage that protects equipment in an emergency.	All DHHI business-units	Ongoing service with notification to local authorities in the event of an emergency.	To ensure all services are compliant, this service must continue operations. In addition to compliance, this service reduces the total impact the organization takes in the event of an emergency.	<A calculated sum of all included personnel and services excluding the initial implementation costs of each individual part of the service. This includes, if applicable, surveillance hardware and software reoccurring costs (costs presented as annual fee), armed security hourly rate multiplied by number of total hours in a year (hourly rate * 8760), climate control system annual rate, and FRS annual rate. This total, excluding initial implementation costs (one-time purchases), will identify the total cost of maintaining this service as expressed through an annual rate.>	<Identify a sample population of industry competitors both with and without the compliance that requires this service to continue operations. Take the average revenue of both parties and subtract the difference in revenue. The calculated difference is an estimate to the amount of revenue gained/lost by being compliant. Also, refer to the Business Impact Analysis (BIA) to identify the cost to recover operations without the current service as well as the cost to recover operations currently. Subtract the two sums and subtract to identify the amount saved by having this service in place. Both figures, the revenue generated by being compliant and the savings accrued by using this security service, are useful in comparing costs if the security service were removed. In addition to calculating these figures, all annual fees will be billed to facilities' budget. >
Data Center - Functional Information System Services	These are the information systems used in business operations to assist in promoting the main mission objectives. These operations can be considered mission objective supplements because of the relationship between these services and the mission objective business functions. While these services are not explicit in generating revenue, these services help in gaining new customers and nurturing relationships with current customers. The servers and their main functions within this security service are identified as the following: server E - DHHI Please Help, server G - DHHI Live, server H - Market-IT, server R - Webz	Marketing department and Information Technology (IT) department (external/internal)	all services must be always kept online, yet support services are required only when needed.	One of DHHI's primary goals is high quality support; therefore, services that provide support either directly through the Please Help system or indirectly through DHHI Live site help accomplish this goal. Other services included that are not related to support are regarding marketing and brand management. As identified in the strategy section of the business plan, name recognition is one of the goals of the organization. To achieve name recognition, services such as Market-IT and Webz are necessary to maintain visibility for potential customers.	<All hardware and software must be calculated to represent an annual cost. In addition to hardware and software, the time (in hours) necessary to provide service to each system must be calculated to a yearly amount; this amount must then be multiplied by the employees (calculate compensation to reflect an hourly rate) responsible for servicing these systems. This is the total cost of maintaining these systems.>	<All customer support will be calculated when deciding the annual rate customers pay (applied to all customers to reduce individual customer expense. All marketing costs which allow for activity metrics (number of new visitors, number of impressions, etc.) can be used to identify the effectiveness of the marketing tool. Subtract the cost of the marketing tools from the number of sales generated to obtain the net cost of the marketing cost. All calculated costs should be billed to the operations department.>

Data Center - Operational Information System Services	These are the systems utilized in the Data Center that help support the organization in achieving its mission objective. These services are not expected to generate revenue; instead, these functions are viewed as the foundational structure that enables the business to continue servicing customers. Within this security service include the following servers and the business function each server is responsible for: server A - Human Resource Information System (HRIS), server B - Payroll system, server C - Account-Master, server F - Mercury Software, server S - Service Now, server U - Domain Name Service (DNS), server V - Outlook 365, and server W - SharePoint.	All DHHI business-units	Continuous, ongoing operation is necessary to support the organizations' goal in achieving mission objectives outlined in business plan.	To ensure the organization can perform the business functions geared toward generating revenue, these operations must be kept online. Critical business operations regarding communication (internal and external), finance (human resources and accounts payable), and system information (configuration settings and domain name functionality) are all included in this service; therefore, unless otherwise directed by leadership, these systems must remain online and serviced as needed.	<All hardware and software must be calculated to represent an annual cost. In addition to hardware and software, the time (in hours) necessary to provide service to each system must be calculated to a yearly amount; this amount must then be multiplied by each member involved in the services using the member's compensation calculated to represent hourly pay rate. The total sum of all these elements represents the cost associated with this service.>	<Servers A, B, C, and F's expenses (hardware, software, and man hours) will be billed to the finance department. Servers S, U, V, and W's expenses (hardware, software, and man hours) will be billed to the operations department.>
Data Center - Managerial Information Security Services	These are the systems utilized in the Data Center that assist leadership in making strategic and/or executive decisions regarding the organization. Within this security service includes Server D, Regu-Nation, and Server Q, Archer RSA.	Upper Management (.i.e., Managers, Leadership, Board of Directors, etc.)	Continuous, ongoing operation to produce real time results to constituency.	Both servers report information that management can reference when making strategic and/or executive decisions. Without this information, management has the risk of making ill-informed decisions, leading the organization down a potential path including: loss in the form of fines accrued from regulations not made aware to the company; improper communication of data disclosures to customers that leads to losses from class action lawsuits because an incident was not reported; the organization continuing a business function despite increased regulation in that sector to which it cannot effectively compete with other parties resulting in a missed opportunity.	<The total cost of this service requires a summation of all components of both servers including hardware costs, software costs, network costs, and operational costs of maintaining the servers. The servers can be calculated by identifying the cost of each server as well as identifying the mean time to replace (MTTR) to calculate the time each server will last on average. Take this time and perform a proportional equation to identify the annual rates for maintaining each server. Each software should have a fee; take this fee and calculate the total rate of both software systems. The operational costs can be calculated by identifying the average time spent on maintenance for each server in a month. Multiply this time by the hourly rate calculated from each employee involved in the maintenance. This total will then be multiplied by 12 to calculate the annual fee of maintaining operations. >	Reference the Business Impact Assessment (BIA) performed on each system to identify the costs of removing each system. Subtract the expenditure with the calculated amount to identify any savings accrued by maintaining operations. All annual expenses identified in the expenditure column will be billed to upper management to cover the costs.

Summary

Implementation Strategy

To ensure that the directory included all services utilized by the organization, research was performed by referencing the Diamond Hands Holdings Inc. (DHHI) business plan as well as the DHHI policy and planning omnibus. In reviewing the documents, any service control category (technical, operational, or managerial) that performs some action (planning, monitoring, developing, implementing, etc.) related to the Confidentiality, Integrity, and Availability (CIA) triad was identified as a security service; thus, that service was included in the security services directory.

Limitations

Due to the natural limitations in this project, this plan was developed and documented in a classroom setting as opposed to an actual business setting, the security services directory deliverable does not contain all the information available that may be seen in one created in a professional, business environment. Should this project have been performed in a professional, business environment, there would be additional action items that would have been taken to ensure the information identified in the security services directory was done so with a high level of confidence regarding accuracy. Such action items that would have been performed include performing additional research on company systems to ensure all information systems, including those potentially not added to the documents referenced earlier, are included in the directory.

Plan Validation

If business-unit partners were available for consultation, this plan could be further validated by ensuring the information regarding each security service was entered correctly as approved by the appropriate member of each individual responsible for the security service in question. In addition to reviewing information about each security service with the responsible party, additional interviews involving all members of a system or process (system/process owner, functional user, administrator, etc.) would take place to ensure this service in question is correctly identified as a security service according to the criteria outlined in the earlier section. In these interviews, there will also be questions asked to help identify more information for each data point of the service (cost, cost recovery, justification, frequency, etc.).

REFERENCES

Bowen, P., Hash, J., & Wilson, M. (2006). *Information Security Handbook: A Guide for Managers* (NIST SP 800-100). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-100

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/Eal4er0l6ABAlNX4Vj5eXHUBVjwvLzxFAw2M0BvOXYEUqQ?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

Council, T. S. E. (2018, August 18). *Defending your budget*. SEC. Retrieved October 21, 2021, from https://www.securityexecutivecouncil.com/spotlight/index.html?sid=30102.

Grance, T., Hash, J., Stevens, M., O'Neal, K., & Bartol, N. (2003). *Guide to information technology security services* (NIST SP 800-35; 0 ed., p. NIST SP 800-35). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-35

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security* (NIST SP 800-12r1; p. NIST SP 800-12r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1