Risk Assessment of:

H.R. Swisher Manufacturing Incorporated

Conducted by: Jeffrey Yang

April 14, 2020

Contents

[Executive Summary 3](#_Toc37801647)

[Process 1 5](#_Toc37801648)

[Worksheet W1.1 Senior Management Important Assets 5](#_Toc37801649)

[Worksheet W1.3 Senior Management Security Requirements 6](#_Toc37801650)

[Worksheet W1.4 Senior Management Survey 7](#_Toc37801651)

[President and CEO 7](#_Toc37801652)

[V.P. for Sales – North America 12](#_Toc37801653)

[Site Manager 17](#_Toc37801654)

[Worksheet W1.5 Senior Management Protection Strategy 22](#_Toc37801655)

[Process 2 24](#_Toc37801656)

[Worksheet W2.1 Operational Management Important Assets 24](#_Toc37801657)

[Worksheet W2.3 Operational Management Security Requirements 26](#_Toc37801658)

[Plant Production Manager 28](#_Toc37801659)

[Site Safety Manager 33](#_Toc37801660)

[Engineering Manager 38](#_Toc37801661)

[Site Accounting Manager 43](#_Toc37801662)

[Human Resources Manager 48](#_Toc37801663)

[Worksheet W2.5 Operational Management Protection Strategy 53](#_Toc37801664)

[Process 3 56](#_Toc37801665)

[Worksheet W3.1 Operational Staff Important Assets 56](#_Toc37801666)

[Worksheet W3.3 Operational Staff Security Requirements 57](#_Toc37801667)

[Worksheet W3.4 Operational Staff Survey 58](#_Toc37801668)

[Secretary to Site Manager 58](#_Toc37801669)

[Inventory Planning and Purchasing Agent 63](#_Toc37801670)

[Production Engineer 68](#_Toc37801671)

[Production Worker 73](#_Toc37801672)

[Worksheet W3.5 Operational Staff Protection Strategy 78](#_Toc37801673)

[Process 3A 80](#_Toc37801674)

[Worksheet W3a.1 IT Staff Important Assets 80](#_Toc37801675)

[Worksheet W3a.3 IT Staff Security Requirements 81](#_Toc37801676)

[Worksheet W3a.4 IT Staff Survey 82](#_Toc37801677)

[IT Administrator 82](#_Toc37801678)

[Worksheet W3a.5 IT Staff Protection Strategy 91](#_Toc37801679)

[Process 4 92](#_Toc37801680)

[Worksheet W4.1 Asset Group Worksheet 92](#_Toc37801681)

[Top Five Critical Assets 95](#_Toc37801682)

[Asset Workbooks 96](#_Toc37801683)

[Production System 96](#_Toc37801684)

[Production System Worksheet A4.1 Critical Asset Information 96](#_Toc37801685)

[Production System Worksheet A4.2 Security Requirements Group Worksheet 97](#_Toc37801686)

[Production System Worksheet W4.2 Security Requirements Group Worksheet 98](#_Toc37801687)

[Production System Worksheet W4.3 Areas of Concern 99](#_Toc37801688)

[Production System Worksheet A4.3 Threat Trees 103](#_Toc37801689)

[Production System Worksheet A5.1 Identify Key Classes of Components 107](#_Toc37801690)

[Production System Worksheet A5.2 Identify Infrastructure Components to Examine 108](#_Toc37801691)

[Production System Worksheet A6.1 Review Technology Vulnerabilities and Summarize Results 113](#_Toc37801692)

[Production System Worksheet A7.1 Identify the Impact of Threats to Critical Assets 116](#_Toc37801693)

[Production System Worksheet A7.2 Create Risk Evaluation Criteria 124](#_Toc37801694)

[Production System Worksheet A7.3 Evaluate the Impacts of Threats to Critical Assets 126](#_Toc37801695)

[Scheduling Data 130](#_Toc37801696)

[Scheduling Data Worksheet A4.1 Critical Asset Information 130](#_Toc37801697)

[Scheduling Data Worksheet A4.2 Security Requirements Group Worksheet 131](#_Toc37801698)

[Scheduling Data Worksheet W4.2 Security Requirements Group Worksheet 132](#_Toc37801699)

[Scheduling Data Worksheet W4.3 Areas of Concern 133](#_Toc37801700)

[Scheduling Data Worksheet A4.3 Threat Trees 136](#_Toc37801701)

[Scheduling Data Worksheet A5.1 Identify Key Classes of Components 141](#_Toc37801702)

[Scheduling Data Worksheet A5.2 Identify Infrastructure Components to Examine 142](#_Toc37801703)

[Scheduling Data Worksheet A6.1 Review Technology Vulnerabilities and Summarize Results 145](#_Toc37801704)

[Scheduling Data Worksheet A7.1 Identify the Impact of Threats to Critical Assets 147](#_Toc37801705)

[Scheduling Data Worksheet A7.2 Create Risk Evaluation Criteria 155](#_Toc37801706)

[Scheduling Data Worksheet A7.3 Evaluate the Impacts of Threats to Critical Assets 157](#_Toc37801707)

[Research and Development Data 161](#_Toc37801708)

[Research and Development Data Worksheet A4.1 Critical Asset Information 161](#_Toc37801709)

[Research and Development Data Worksheet A4.2 Security Requirements Group Worksheet 162](#_Toc37801710)

[Research and Development Data Worksheet W4.2 Security Requirements Group Worksheet 163](#_Toc37801711)

[Research and Development Data Worksheet W4.3 Areas of Concern 164](#_Toc37801712)

[Research and Development Data Worksheet A4.3 Threat Trees 167](#_Toc37801713)

[Research and Development Data Worksheet A5.1 Identify Key Classes of Components 172](#_Toc37801714)

[Research and Development Data Worksheet A5.2 Identify Infrastructure Components to Examine 173](#_Toc37801715)

[Research and Development Data Worksheet A6.1 Review Technology Vulnerabilities and Summarize Results 177](#_Toc37801716)

[Research and Development Data Worksheet A7.1 Identify the Impact of Threats to Critical Assets 179](#_Toc37801717)

[Research and Development Data Worksheet A7.2 Create Risk Evaluation Criteria 187](#_Toc37801718)

[Research and Development Data Worksheet A7.3 Evaluate the Impacts of Threats to Critical Assets 189](#_Toc37801719)

[Inventory System 193](#_Toc37801720)

[Inventory System Worksheet A4.1 Critical Asset Information 193](#_Toc37801721)

[Inventory System Worksheet A4.2 Security Requirements Group Worksheet 194](#_Toc37801722)

[Inventory System Worksheet W4.2 Security Requirements Group Worksheet 195](#_Toc37801723)

[Inventory System Worksheet W4.3 Areas of Concern 196](#_Toc37801724)

[Inventory System Worksheet A4.3 Threat Trees 199](#_Toc37801725)

[Inventory System Worksheet A5.1 Identify Key Classes of Components 203](#_Toc37801726)

[Inventory System Worksheet A5.2 Identify Infrastructure Components to Examine 204](#_Toc37801727)

[Inventory System Worksheet A6.1 Review Technology Vulnerabilities and Summarize Results 208](#_Toc37801728)

[Inventory System Worksheet A7.1 Identify the Impact of Threats to Critical Assets 210](#_Toc37801729)

[Inventory System Worksheet A7.2 Create Risk Evaluation Criteria 218](#_Toc37801730)

[Inventory System Worksheet A7.3 Evaluate the Impacts of Threats to Critical Assets 220](#_Toc37801731)

[IT Staff 224](#_Toc37801732)

[IT Staff Worksheet A4.1 Critical Asset Information 224](#_Toc37801733)

[IT Staff Worksheet A4.2 Security Requirements Group Worksheet 225](#_Toc37801734)

[IT Staff Worksheet W4.2 Security Requirements Group Worksheet 226](#_Toc37801735)

[IT Staff Worksheet W4.3 Areas of Concern 227](#_Toc37801736)

[IT Staff Worksheet A4.3 Threat Trees 230](#_Toc37801737)

[IT Staff Worksheet A5.1 Identify Key Classes of Components 235](#_Toc37801738)

[IT Staff Worksheet A5.2 Identify Infrastructure Components to Examine 236](#_Toc37801739)

[IT Staff Worksheet A6.1 Review Technology Vulnerabilities and Summarize Results 239](#_Toc37801740)

[IT Staff Worksheet A7.1 Identify the Impact of Threats to Critical Assets 241](#_Toc37801741)

[IT Staff Worksheet A7.2 Create Risk Evaluation Criteria 249](#_Toc37801742)

[IT Staff Worksheet A7.3 Evaluate the Impacts of Threats to Critical Assets 251](#_Toc37801743)

[Process 8A 255](#_Toc37801744)

[Process W8A.1 Current Protection Strategy 255](#_Toc37801745)

[Process W8A.2 Current Operational Practices 267](#_Toc37801746)

[Process W8A.3 Protection Strategy for Strategic Practices 287](#_Toc37801747)

[Process W8A.4 Protection Strategy for Operational Practices 293](#_Toc37801748)

[Process A8.3 Mitigation Plans 296](#_Toc37801749)

[Process W8A.5 Action List 300](#_Toc37801750)

[References 303](#_Toc37801751)

# Executive Summary

A detailed risk assessment of H.C. Swisher Manufacturing’s information systems and what their important assets are, what the risks are associated with those assets, and what mitigation plans were developed to help prevent those risks from materializing.

Initially, Swisher did not have a proper IT staff on the premise, relying solely on third-party IT services. The issue was that these individuals did not understand the processes of Swisher's systems, such as their production system, and would refuse to check issues related to it. These individuals did not follow best practices, and hence, did not have Swisher's best interest. Since then, an IT administrator has been hired and has redone the IT systems and network to a functional state. However, there were still a few risks that were discovered through the use of interviews and surveys.

Initial testing was interviews given out to individuals based on their organizational group. This allows a company-wide view of the interests and what each organizational level/individual of said group viewed as critical assets. The interviews looked to extract information determining the most important assets that said individual thought was most important. These interviews showed us that administrative managers were more concerned with administrative tasks and information that could cause major financial harm to their company. The operational managers were focused on their staff and the assets that mostly pertained to the management of their staff. The staff's important assets were anything that had any impact on their daily routine. IT staff is primarily focused on the IT systems and network of the company. The second test was distributed as surveys, with predefined questions on how well the interviewed individuals understood the policies, procedures, and roles and responsibilities in the organization concerning information assets.

The information in the interviews is then processed, into the top five most important assets to Swisher. These five assets were chosen by cross-referencing how many times they were mentioned as an asset in the interviews. The top five assets are:

* Production System
* Scheduling Data
* Research and Development Data
* Inventory System
* IT Staff

These five assets are the most important and thus the risk assessment puts a focus on. The top five assets were put through a security test, defining the requirements of confidentiality, integrity, and availability and determining which one has the highest priority for each asset. Areas of concern were then recorded for each of the five assets by groups according to the organizational level. With this knowledge, the five assets were put into threat trees, which showed the possible ways that a threat could disclose, modify, destroy, or interrupt one of the critical assets. These were done through human actors either using network or physical access, system issues, and other related issues.

The assets then were analyzed and put into systems of interest. This just shows which systems that the asset is most closely related to in its operation. Software and hardware components were then analyzed, for they are possible risk points that need to be addressed. These included servers, networking and security components, etc. For the IT staff critical asset, which is neither software or hardware, but rather an entity, a separate class of components was made specifically for them. These components were aimed at possible ways of disclosure of IT staff information and possible unavailability. Once this information was gathered, audit criteria were generated to test each of the components for vulnerabilities. The audits were then performed. With the gathered information from the audits, Swisher’s vulnerabilities could be determined. Action and recommendation plans were written as to how to address these vulnerabilities.

Next, further analysis of the five assets were made, specifically in terms of disclosure, modification, destruction/loss, and interruption. Questions concerning Swisher’s reputation, customer confidence, legal penalties, etc., were asked of each asset. These were then ranked by a risk level of high, medium, and low. Additionally, the threat trees from earlier are then updated to contain the impacts to Swisher, by high, medium, and low.

Finally, all the survey answers from earlier were consolidated into tables, and protection practices and vulnerabilities were described by each organizational group. With this information, and even more in-depth protection strategy was developed, for each strategic practice that was in the survey. During the development of the protection strategies, mitigation plans were made for the five assets. These looked into what actions Swisher should take to protect their assets from human actors using the network and physical access, system issues, and other issues.

In the end, an action list was created, with specific action plans that Swisher should take to improve the level of security their company has and to reduce their level of risk. The action lists take a look into what should be done with 30, 60, 90, 180 and 365 days from the receiving date of this assessment. The actions list includes additional training for staff as well as an awareness campaign to be developed. Additional hires for the IT staff, the use of encryption software, physical protection for hardware, among others. Swisher can expect to reduce the level of risk that their IT systems take on if they follow the action list plans in their given time frame.

# Process 1

## Worksheet W1.1 Senior Management Important Assets

|  |
| --- |
| Assets |
| 1. What are your important assets?  * Own/partner’s intellectual property * Production process/data * Manufacturing systems hardware/controllers * Client data * Engineers * Product pricing data and client contracts * Ordering and shipping systems * Research and development data * Inventory data * Scheduling data * IT administrator |
| 1. Are there any other assets that you are required to protect (e.g., by law or regulation)?  * Credit card transactions through PCI DSS * Intellectual property laws * Privacy Act of 1974 |
| 1. What related assets are important?  * On-site computer systems * Supplier connection * Reputation * IT administrator relationship * Interns * Client/employee personally identifiable information |
| 1. From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?  * **Intellectual Property** – Swisher works in a very niche field and they need all the competitive edge they need. Stolen IP can result in loss business to competitors. There is also IP laws in place that Swisher needs to be in compliance with. * **Client Data** – Client information is a critical asset because it can be a breach of a multitude of laws and regulations, depending on the type leaked. One such law is PCI DSS which deals with credit card transactions. * **Research and Development Data** – This is very important as Swisher creates custom products for clients. This data cannot be leaked to the public as their competitors may take it and steal their clients. |

## Worksheet W1.3 Senior Management Security Requirements

|  |
| --- |
| Security Requirements |
| 1. What are the important security requirements for each information asset?  * **Intellectual Property**   + *Confidentiality* – IP should be kept confidential due to IP laws; Privacy Act of 1974.   + *Integrity* – Only authorized personnel can read or write to the data.   + *Availability* – Should be available to authorized personnel only when given permission. * **Client Data**   + *Confidentiality* – Information should be kept confidential; Privacy Act of 1974.   + *Integrity* – Only authorized personnel can read the data.   + *Availability* - Should be available to authorized personnel only when given permission. * **Research and Development Data**   + *Confidentiality* – R&D data should be kept within Swisher and kept confidential.   + *Integrity* – Only authorized personnel can read or write to the data.   + *Availability -* Should be available to authorized personnel only when given permission. |
| 1. What is the relative ranking of the security requirements for each information asset?   Which security requirement is the most important?   * **Intellectual Property**   1. **Confidentiality**   2. Integrity   3. Availability * **Client Data**   1. **Confidentiality**   2. Availability   3. Integrity * **Research and Development Data**   1. **Confidentiality**   2. **Integrity**   3. Availability |

## Worksheet W1.4 Senior Management Survey

### President and CEO

Name: Tyrell Wellick

Position: President and CEO

| Senior Management Survey | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| Security Awareness and Training | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | **Yes** No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | **Yes**  No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | **Yes**  No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes **No**  Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | **Yes** No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | **Yes**  No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes **No** Don’t  Know |

| Senior Management Survey (cont.) | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Management (cont.)** | |
| Security roles and responsibilities are defined for all staff in the organization. | **Yes** No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes **No** Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | **Yes** No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No **Don’t**  **Know** |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | **Yes** No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No **Don’t**  **Know** |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes **No** Don’t  Know |
| The organization uniformly enforces its security policies. | **Yes** No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | **Yes** No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes **No** Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No **Don’t**  **Know** |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | **Yes** No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | **Yes** No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No **Don’t**  **Know** |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes **No** Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes **No** Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No **Don’t**  **Know** |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | **Yes** No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | **Yes** No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | **Yes** No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes **No** Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | **Yes** No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes **No** Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes **No** Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes No **Don’t**  **Know** |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes **No** Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No **Don’t**  **Know** |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes **No** Don’t  Know |

### V.P. for Sales – North America

Name: Angela Moss

Position: V.P. for Sales in North America

| Senior Management Survey | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| Security Awareness and Training | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | **Yes** No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | **Yes** No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Yes No **Don’t**  **Know** |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | **Yes** No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | **Yes** No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes **No** Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | **Yes** No Don’t  Know |

| Senior Management Survey (cont.) | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Management (cont.)** | |
| Security roles and responsibilities are defined for all staff in the organization. | **Yes** No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | **Yes** No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | **Yes** No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No **Don’t**  **Know** |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | **Yes** No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes **No** Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No **Don’t**  **Know** |
| The organization uniformly enforces its security policies. | **Yes** No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | **Yes** No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | **Yes** No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes **No** Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | **Yes** No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | **Yes** No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | **Yes** No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | **Yes** No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes **No** Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | **Yes** No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No **Don’t**  **Know** |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No **Don’t**  **Know** |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | **Yes** No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | **Yes** No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | **Yes** No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | **Yes** No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | **Yes** No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | **Yes** No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No **Don’t**  **Know** |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | **Yes** No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No **Don’t**  **Know** |

### Site Manager

Name: Phillip Price

Position: Site Manager

| Senior Management Survey | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| Security Awareness and Training | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | **Yes** No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes No **Don’t**  **Know** |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Yes No **Don’t**  **Know** |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | **Yes** No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | **Yes** No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | **Yes** No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | **Yes** No Don’t  Know |

| Senior Management Survey (cont.) | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Management (cont.)** | |
| Security roles and responsibilities are defined for all staff in the organization. | **Yes** No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | **Yes** No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | **Yes** No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes No **Don’t**  **Know** |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | **Yes** No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | **Yes** No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes **No** Don’t  Know |
| The organization uniformly enforces its security policies. | **Yes** No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes **No** Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | **Yes** No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | **Yes** No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No **Don’t**  **Know** |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes **No** Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No **Don’t**  **Know** |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | **Yes** No Don’t  Know |
| There are documented policies and procedures for managing visitors. | **Yes** No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | **Yes** No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | **Yes** No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No **Don’t**  **Know** |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes No **Don’t**  **Know** |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes **No** Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | **Yes** No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | **Yes** No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | **Yes** No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | **Yes** No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes **No** Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | **Yes** No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes No **Don’t**  **Know** |

## Worksheet W1.5 Senior Management Protection Strategy

| Protection Strategy |
| --- |
| 1. Which issues from the survey would you like to discuss in more detail?   **President & CEO**   * Physical security plans and procedures. * Incident management. * General staff practices.   **V.P. for Sales – NA**   * Security policies and regulations. * Physical access control. * General staff practices.   **Site Manager**   * Security awareness and training. * Contingency planning/disaster recovery. * System and network management. |
| 1. What important issues did the survey not cover?   **President & CEO**   * Do not know where our client data concerning credit cards go. The servicing bank says the they are compliant.   **V.P. for Sales – NA**   * Sales staff might be talking about our contacts with competitor’s sales staff.   **Site Manager**   * Personnel safety. * Data backups. * Inventory and scheduling system failures. Leads to use of wrong materials by staff who know not to use them. |
| 1. Are there specific security policies, procedures, and practices unique to certain assets? What are they?   **President & CEO**   * Engineers are required to sign a three-year non-competition agreement in case they want to leave Swisher.   **V.P. for Sales – NA**   * Estimate first and second year sales volume and pricing which determines the terms of the contract. * Download product information to sales personnel’s laptop before visiting clients.   **Site Manager**   * N/A |
| 1. Do you think that your organization’s protection strategy is effective?   How do you know?  **President & CEO**   * Yes – All staff are trained and understand their security roles and responsibilities. Swisher has not lost any intellectual property of our own or clients. Our client’s credit card data is safe as well, according to our servicing bank.   **V.P. for Sales – NA**   * Yes – All staff are trained and should understand their security roles and responsibilities.   **Site Manager**   * No – All the research and development data sit on the computer systems on-site. No idea if the data is backed up or not either. |

# Process 2

## Worksheet W2.1 Operational Management Important Assets

|  |
| --- |
| Assets |
| 1. What are your important assets?  * Production process/data * Scheduling data * Manufacturing systems hardware/controllers * Engineers * IT administrator * Inventory data * IoT cameras and collected data (separate network) * Design system (separate network) * Research and development data * Own intellectual property * Backup systems * Time card/payroll records * Accounts payable/receivable data * Ordering and shipping system * Personnel data |
| 1. Are there any other assets that you are required to protect (e.g., by law or regulation)?  * OSHA (Occupational Safety and Health Administration) standards * Intellectual property laws * Privacy Act of 1974 * GAAP (Generally Accepted Accounting Principles) |
| 1. What related assets are important?  * Staff health and safety * Alarm system * Monitoring system * Physical security * Accounting systems * Billing system |
| 1. From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?  * **Production Process/Data** – Production is the primary processes that Swisher needs to go through to produce products for their clients. Delays from automated systems could cause loss of future sales. * **Monitoring System** – Safety of staff members as well as general grounds monitoring prevents liabilities for Swisher. The system is on its own network with IoT cameras, as to prevent hackers from jumping from their monitoring system to their primary network. * **Research and Development Data** - This is very important as Swisher creates custom products for clients. This data cannot be leaked to the public as their competitors may take it and steal their clients. Alteration of R&D data could set back productivity by weeks or months as it may have to be reconstructed from scratch. * **Ordering/Shipping System** – The right materials need to be ordered for products to be produced. The use of wrong materials will produce inferior products, or if delayed, will push back delivery of products to clients by weeks or months. * **Personnel Data** – The primary concern with personnel data is that it keeps its integrity. This includes Personally Identifiable Information, to which should only be available to HR staff. |

## Worksheet W2.3 Operational Management Security Requirements

|  |
| --- |
| Security Requirements |
| 1. What are the important security requirements for each information asset?  * **Production Process/Data**   + *Confidentiality* – Should be kept confidential to retain competitive edge against other companies in the same market.   + *Integrity* – Only authorized personnel can read or write to the data.   + *Availability* – System should be available during work hours to authorized personnel. * **Monitoring System**   + *Confidentiality* – Should be kept confidential due to the fact that these provide recordings of individuals and the property.   + *Integrity* – Ensure that the monitoring system is not altered with to prevent proper functionality.   + *Availability* – Should be available 24/7 to authorized personnel. * **Research and Development Data**   + *Confidentiality* – R&D data should be kept within Swisher and kept confidential.   + *Integrity* – Only authorized personnel can read or write to the data.   + *Availability* – Should be available to authorized personnel only when given permission. * **Ordering/Shipping System**   + *Confidentiality* – Should be kept confidential to prevent knowledge of materials used to competitors.   + *Integrity* – Only authorized personnel should be able to change orders and shipments of material.   + *Availability* – Should be available 24/7 to authorized personnel. * **Personnel Data**   + *Confidentiality* – Should be kept confidential as to prevent PII from being released.   + *Integrity* – Only authorized personnel can read or write to the data.   + *Availability* – Should be available 24/7 to authorized personnel. |
| 1. What is the relative ranking of the security requirements for each information asset?   Which security requirement is the most important?   * **Production Process/Data**   1. **Availability**   2. Confidentiality   3. Integrity * **Monitoring System**   1. **Availability**   2. **Confidentiality**   3. Integrity * **Research and Development Data**   1. **Confidentiality**   2. **Integrity**   3. Availability * **Ordering/Shipping System**   1. **Availability**   2. **Integrity**   3. Confidentiality * **Personnel Data**   1. **Confidentiality**   2. Integrity   3. Availability |

Worksheet W2.4 Operational Management Survey

### Plant Production Manager

Name: Takeshi Kovacs

Position: Plant Production Manager

| Operational Area Management Survey | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No **Don’t**  **Know** |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | **Yes** No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Yes **No** Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes No **Don’t**  **Know** |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | **Yes** No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes **No** Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes **No** Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | **Yes** No Don’t  Know |

| Operational Area Management Survey (cont.) | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Management (cont.)** | |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes **No** Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes **No** Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes **No** Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | **Yes** No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes No **Don’t**  **Know** |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes **No** Don’t  Know |
| The organization uniformly enforces its security policies. | Yes **No** Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | **Yes** No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | **Yes** No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | **Yes** No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No **Don’t**  **Know** |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | **Yes** No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | **Yes** No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | **Yes** No Don’t  Know |
| There are documented policies and procedures for managing visitors. | **Yes** No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | **Yes** No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No **Don’t**  **Know** |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No **Don’t**  **Know** |
| **Monitoring and Auditing Physical Security** | |
| Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed. | Yes **No** Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | **Yes** No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | **Yes** No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | **Yes** No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | **Yes** No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No **Don’t**  **Know** |
| There are documented policies and procedures for working with law enforcement agencies. | Yes **No** Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No **Don’t**  **Know** |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes **No** Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes **No** Don’t  Know |

### Site Safety Manager

Name: Kristin Ortega

Position: Site Safety Manager

| Operational Area Management Survey | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | **Yes** No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | **Yes** No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Yes No **Don’t**  **Know** |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | **Yes** No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes No **Don’t**  **Know** |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | **Yes** No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | **Yes** No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes **No** Don’t  Know |

| Operational Area Management Survey (cont.) | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Management (cont.)** | |
| The organization’s hiring and termination practices for staff take information security issues into account. | **Yes** No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | **Yes** No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes **No** Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | **Yes** No Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | **Yes** No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes **No** Don’t  Know |
| The organization uniformly enforces its security policies. | Yes **No** Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes **No** Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | **Yes** No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No **Don’t**  **Know** |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | **Yes** No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes **No** Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | **Yes** No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | **Yes** No Don’t  Know |
| There are documented policies and procedures for managing visitors. | **Yes** No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes **No** Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No **Don’t**  **Know** |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes No **Don’t**  **Know** |
| **Monitoring and Auditing Physical Security** | |
| Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed. | **Yes** No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | **Yes** No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | **Yes** No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | **Yes** No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes **No** Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No **Don’t**  **Know** |
| There are documented policies and procedures for working with law enforcement agencies. | **Yes** No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | **Yes** No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes **No** Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | **Yes** No Don’t  Know |

### Engineering Manager

Name: Reileen Kawahara

Position: Engineering Manager

| Operational Area Management Survey | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes **No** Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes **No** Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | **Yes** No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes **No** Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes **No** Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes **No** Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | **Yes** No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | **Yes** No Don’t  Know |

| Operational Area Management Survey (cont.) | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Management (cont.)** | |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes **No** Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes **No** Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | **Yes** No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes **No** Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes **No** Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | **Yes** No Don’t  Know |
| The organization uniformly enforces its security policies. | **Yes** No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes **No** Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | **Yes** No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | **Yes** No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No **Don’t**  **Know** |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes No **Don’t**  **Know** |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes **No** Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes **No** Don’t  Know |
| There are documented policies and procedures for managing visitors. | **Yes** No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No **Don’t**  **Know** |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | **Yes** No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | **Yes** No Don’t  Know |
| **Monitoring and Auditing Physical Security** | |
| Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed. | **Yes** No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes **No** Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes **No** Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | **Yes** No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | **Yes** No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes **No** Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | **Yes** No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No **Don’t**  **Know** |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | **Yes** No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes **No** Don’t  Know |

### Site Accounting Manager

Name: James Holden

Position: Site Accounting Manager

| Operational Area Management Survey | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | **Yes** No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | **Yes** No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Yes **No** Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes No **Don’t**  **Know** |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | **Yes** No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | **Yes** No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes **No** Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | **Yes** No Don’t  Know |

| Operational Area Management Survey (cont.) | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Management (cont.)** | |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes **No** Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | **Yes** No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Yes **No** Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes **No** Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | **Yes** No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes No **Don’t**  **Know** |
| The organization uniformly enforces its security policies. | **Yes** No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes **No** Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes **No** Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | **Yes** No Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes **No** Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes **No** Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes No **Don’t**  **Know** |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | **Yes** No Don’t  Know |
| There are documented policies and procedures for managing visitors. | **Yes** No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes **No** Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | **Yes** No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | **Yes** No Don’t  Know |
| **Monitoring and Auditing Physical Security** | |
| Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed. | Yes **No** Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | **Yes** No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes **No** Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes No **Don’t**  **Know** |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes **No** Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | **Yes** No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | **Yes** No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes **No** Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes **No** Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | **Yes** No Don’t  Know |

### Human Resources Manager

Name: Alex Kamal

Position: Site Human Resources Manager

| Operational Area Management Survey | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | **Yes** No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | **Yes** No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | **Yes** No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | Yes **No** Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes **No** Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | **Yes** No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | **Yes** No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | **Yes** No Don’t  Know |

| Operational Area Management Survey (cont.) | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Management (cont.)** | |
| The organization’s hiring and termination practices for staff take information security issues into account. | **Yes** No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes **No** Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | **Yes** No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes No **Don’t**  **Know** |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | **Yes** No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | Yes **No** Don’t  Know |
| The organization uniformly enforces its security policies. | **Yes** No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No **Don’t**  **Know** |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes No **Don’t**  **Know** |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes **No** Don’t  Know |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes No **Don’t**  **Know** |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | **Yes** No Don’t  Know |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes **No** Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | **Yes** No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes **No** Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | **Yes** No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No **Don’t**  **Know** |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | **Yes** No Don’t  Know |
| **Monitoring and Auditing Physical Security** | |
| Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed. | Yes **No** Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes No **Don’t**  **Know** |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | **Yes** No Don’t  Know |
| **Authentication and Authorization** | |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | **Yes** No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | **Yes** No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | **Yes** No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes **No** Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes **No** Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | **Yes** No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | **Yes** No Don’t  Know |

## Worksheet W2.5 Operational Management Protection Strategy

| Protection Strategy |
| --- |
| 1. Which issues from the survey would you like to discuss in more detail?   **Plant Production Manager**   * Security management * Security policies and regulations * General staff practices   **Site Safety Manager**   * Security policies and regulations * Physical access control * Authentication and authorization   **Engineering Manager**   * Contingency planning/disaster recovery * Security strategy * System and network management   **Site Accounting Manager**   * Security management * Security policies and regulations * Contingency planning/disaster recovery   **Site HR Manager**   * Security strategy * Collaborative security management * Contingency planning/disaster recovery |
| 1. What important issues did the survey not cover?   **Plant Production Manager**   * Production system is automated and receives instructions from the schedule system. If something is wrong, then substitute material is used to keep production going.   **Site Safety Manager**   * Health and safety of the workers.   **Engineering Manager**   * A clean desk policy.   **Site Accounting Manager**   * The accounting system gets information from the inventory system, and staff that rush may forget to complete a receipt when placing orders. They may forget for weeks at a time, in which my team cannot send out a bill.   **Site HR Manager**   * N/A |
| 1. Are there specific security policies, procedures, and practices unique to certain assets? What are they?   **Plant Production Manager**   * Production system gets instructions directly from the scheduling system.   **Site Safety Manager**   * Every employee is trained on how to respond in case of an emergency.   **Engineering Manager**   * The entire lab system should be for authorized personnel ONLY. * No simulation can be left running through the weekend.   **Site Accounting Manager**   * N/A   **Site HR Manager**   * N/A |
| 1. Do you think that your organization’s protection strategy is effective?   How do you know?  **Plant Production Manager**   * Yes – With the new IT administrator we hired, she has taken care of essentially all of my security concerns.   **Site Safety Manager**   * Yes – Working for the past 20 years and nothing majorly wrong has happened.   **Engineering Manager**   * No – People that are not supposed to be in the labs are always in here.   **Site Accounting Manager**   * Yes – Have not had an issue with leaked time card and payroll records. Same with accounts payable and receivables.   **Site HR Manager**   * Yes – The IT administrator does all the security that I need. My data is backed up and secure. |

# Process 3

## Worksheet W3.1 Operational Staff Important Assets

|  |
| --- |
| Assets |
| 1. What are your important assets?  * Office systems * Scheduling system * IT administrator * Scheduling data * Inventory data * Ordering and shipping systems * Production network * Production computers |
| 1. Are there any other assets that you are required to protect (e.g., by law or regulation)?  * OSHA |
| 1. What related assets are important?  * Office applications * E-mail * Calendars * Reputation * Vendor information * Administrative network * Data network * Control console * Terminals |
| 1. From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?  * **Scheduling Data** – This is important because it shows the progress of the product and when it is ready for shipment. If the scheduled date is missed, then Swisher could lose a client. The schedule also allows inventory to order materials on time. * **Inventory Data** – Inventory data contains the information that orders the materials to build products for clients. If material isn’t ordered in time, it can set back the delivery date, or in some instances, wrong material may end up being used, creating an inferior product. * **Production Network** – The production network contains all the production computers which have production programs on them. These programs tell the machines what to build, and if correct, then automation takes over. If something is wrong in the production program, then it could waste a bunch of material. * **IT Administrator** – The IT administrator essentially allows the entire company to operate. She ensures the office systems such as computers and other appliances function properly. She also keeps the inventory system working. She also keeps the production network running so automated tasks do not fail. |

## Worksheet W3.3 Operational Staff Security Requirements

|  |
| --- |
| Security Requirements |
| 1. What are the important security requirements for each information asset?  * **Scheduling Data**   + *Confidentiality* – Should be kept confidential to prevent knowledge of product and material movement from reaching competitors.   + *Integrity* – Only authorized personnel should be able to write to the data.   + *Availability* – Should be available to authorized personnel 24/7. * **Inventory Data**   + *Confidentiality* – Information should be kept confidential to prevent competitors from seeing the materials that Swisher is using for custom builds.   + *Integrity* – Only authorized personnel can read and write to the data.   + *Availability* – Should be available to authorized users when given permission. * **Production Network**   + *Confidentiality* – Should be kept confidential to prevent intellectual property to be released.   + *Integrity* – Only authorized personnel can read and write to the data.   + *Availability* – Should be available to authorized users during operation times. * **IT Administrator**   + *Confidentiality* – Private information should be kept confidential.   + *Integrity* – Ensure personnel is trained to understand company policies.   + *Availability* – Should be available during operation times. |
| 1. What is the relative ranking of the security requirements for each information asset?   Which security requirement is the most important?   * **Scheduling System**   1. **Availability**   2. **Integrity**   3. Confidentiality * **Inventory Data**   1. **Integrity**   2. Confidentiality   3. Availability * **Production Network**   1. **Integrity**   2. **Availability**   3. Confidentiality * **IT Administrator**   1. **Availability**   2. **Integrity**   3. Confidentiality |

## Worksheet W3.4 Operational Staff Survey

### Secretary to Site Manager

Name: Josephus Miller

Position: Secretary of Site Manager

| **Staff Survey** | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes **No** Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes **No** Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | **Yes** No Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | **Yes** No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | **Yes** No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | **Yes** No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes **No** Don’t  Know |

| **Staff Survey (cont.)** | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes **No** Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | **Yes** No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes **No** Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes **No** Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes **No** Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes **No** Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No **Don’t**  **Know** |
| There are documented policies and procedures for physical control of hardware and software. | **Yes** No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes No **Don’t**  **Know** |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes **No** Don’t  Know |
| **System and Network Management** | |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes **No** Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | **Yes** No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes **No** Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes **No** Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes **No** Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes **No** Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes **No** Don’t  Know |

### Inventory Planning and Purchasing Agent

Name: Camina Drummer

Position: Inventory Planning and Purchasing Agent

| **Staff Survey** | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes No **Don’t**  **Know** |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | **Yes** No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Yes **No** Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | **Yes** No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes **No** Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes **No** Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | **Yes** No Don’t  Know |

| **Staff Survey (cont.)** | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes **No** Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes **No** Don’t  Know |
| The organization uniformly enforces its security policies. | Yes **No** Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes **No** Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Yes **No** Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | **Yes** No Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes **No** Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | **Yes** No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | **Yes** No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | **Yes** No Don’t  Know |
| **System and Network Management** | |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes **No** Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | **Yes** No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes No **Don’t**  **Know** |
| There are documented policies and procedures for working with law enforcement agencies. | Yes **No** Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | **Yes** No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | **Yes** No Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes **No** Don’t  Know |

### Production Engineer

Name: Naomi Nagata

Position: Production Engineer

| **Staff Survey** | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes **No** Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | **Yes** No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Yes **No** Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | **Yes** No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | **Yes** No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | **Yes** No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes No **Don’t**  **Know** |

| **Staff Survey (cont.)** | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes **No** Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | **Yes** No Don’t  Know |
| The organization uniformly enforces its security policies. | Yes **No** Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | **Yes** No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | **Yes** No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes **No** Don’t  Know |
| There are documented policies and procedures for managing visitors. | Yes No **Don’t**  **Know** |
| There are documented policies and procedures for physical control of hardware and software. | Yes **No** Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes **No** Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes **No** Don’t  Know |
| **System and Network Management** | |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes No **Don’t**  **Know** |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes No **Don’t**  **Know** |
| Incident management procedures are periodically tested, verified, and updated. | **Yes** No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | Yes **No** Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No **Don’t**  **Know** |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes No **Don’t**  **Know** |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes **No** Don’t  Know |

### Production Worker

Name: Amos Burton

Position: Production Worker

| **Staff Survey** | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | **Yes** No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes **No** Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Yes **No** Don’t  Know |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | **Yes** No Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | Yes **No** Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes **No** Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes **No** Don’t  Know |

| **Staff Survey (cont.)** | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes **No** Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Yes **No** Don’t  Know |
| The organization uniformly enforces its security policies. | Yes **No** Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes No **Don’t**  **Know** |
| **Contingency Planning/Disaster Recovery** | |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | **Yes** No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | **Yes** No Don’t  Know |
| There are documented policies and procedures for managing visitors. | **Yes** No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | Yes No **Don’t**  **Know** |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes **No** Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Yes **No** Don’t  Know |
| **System and Network Management** | |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | Yes **No** Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | **Yes** No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | Yes **No** Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | **Yes** No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | Yes No **Don’t**  **Know** |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes **No** Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes **No** Don’t  Know |

## Worksheet W3.5 Operational Staff Protection Strategy

| Protection Strategy |
| --- |
| 1. Which issues from the survey would you like to discuss in more detail?   **Secretary to the Site Manager**   * Security awareness and training * Incident management * General staff practices   **Inventory Planning and Purchasing Agent**   * Security management * Security policies and regulations * System and network management   **Production Engineer**   * Physical access control * Incident management * General staff practices   **Production Worker**   * Security management * Security policies and regulations |
| 1. What important issues did the survey not cover?   **Secretary to the Site Manager**   * A paper trail that sometimes gets put into the system wrong. IT administrator is the only IT staff for Swisher.   **Inventory Planning and Purchasing Agent**   * Expensive material can be sitting in temporary storage if the scheduling system messes up.   **Production Engineer**   * N/A   **Production Worker**   * Have to have an engineer log in to a terminal to monitor the systems. |
| 1. Are there specific security policies, procedures, and practices unique to certain assets? What are they?   **Secretary to the Site Manager**   * N/A   **Inventory Planning and Purchasing Agent**   * Store a lot of data such as vendor information on own computer in the office, which never leaves the building.   **Production Engineer**   * Production program only begins when safety parameters are checked out.   **Production Worker**   * A security engineer usually leaves their ID and password so we can monitor the system. |
| 1. Do you think that your organization’s protection strategy is effective?   How do you know?  **Secretary to the Site Manager**   * No – Too many people have access to the scheduling system.   **Inventory Planning and Purchasing Agent**   * No – I do not trust the system so I keep vendor information on my computer.   **Production Engineer**   * Yes – Only one major incident in 25 years of working at this company.   **Production Worker**   * Yes – Since the new IT administrator came, we have not had any issues. |

# Process 3A

## Worksheet W3a.1 IT Staff Important Assets

|  |
| --- |
| Assets |
| 1. What are your important assets?  * Production system * Lab system * Administrative system * Network * Scheduling data * Intellectual property |
| 1. Are there any other assets that you are required to protect (e.g., by law or regulation)?  * Privacy Act of 1974 * OSHA |
| 1. What related assets are important?  * Anti-malware packages |
| 1. From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?  * **Production System** – This allows Swisher to produce products for their clients. This is the primary function of Swisher. * **Lab System** – The lab system contains all the intellectual property and research and development data. This is where all the research is done and tested before being pawned off to the production system for production. * **Administrative System** – The administrative system contains all the intellectual property as alongside the lab system. It also contains the information and data that feeds into the production system alongside the lab system. * **Network** – Broken into two logical networks that run the entirety of Swisher. Production and administration. The production system relies on both logical networks to function, and can only operate for a few hours if one or the other is down. |

## Worksheet W3a.3 IT Staff Security Requirements

|  |
| --- |
| Security Requirements |
| 1. What are the important security requirements for each information asset?  * **Production System**   + *Confidentiality* – Should be kept confidential.   + *Integrity* – Only authorized personnel should be able to access the system.   + *Availability* – Should be available to authorized personnel 24/7. * **Lab System**   + *Confidentiality* – Should be kept confidential.   + *Integrity* – Only authorized personnel should be able to access the system.   + *Availability* – Should be available to authorized personnel 24/7. * **Administrative System**   + *Confidentiality* – Should be kept confidential.   + *Integrity* – Only authorized personnel should be able to access the system.   + *Availability* – Should be available to authorized personnel 24/7. * **Network**   + *Confidentiality* – Should be kept confidential.   + *Integrity* – Only authorized personnel should be able to access the system.   + *Availability* – Should be available to authorized personnel 24/7. |
| 1. What is the relative ranking of the security requirements for each information asset?   Which security requirement is the most important?   * **Production System**   1. **Availability**   2. Integrity   3. Confidentiality * **Lab System**   1. **Confidentiality**   2. Integrity   3. Availability * **Administrative System**   1. **Availability**   2. **Integrity**   3. Confidentiality * **Network**   1. **Availability**   2. Integrity   3. Confidentiality |

## Worksheet W3a.4 IT Staff Survey

### IT Administrator

Name: Darlene Alderson

Position: System Administrator

| **IT Staff Survey** | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Awareness and Training** | |
| Staff members understand their security roles and responsibilities. This is documented and verified. | **Yes** No Don’t  Know |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | **Yes** No Don’t  Know |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | **Yes** No Don’t  Know |
| **Security Strategy** | |
| The organization’s business strategies routinely incorporate security considerations. | **Yes** No Don’t  Know |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | **Yes** No Don’t  Know |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | **Yes** No Don’t  Know |

| **IT Staff Survey (cont.)** | |
| --- | --- |
| **Practice** | **Is this practice used by your organization?** |
| **Security Management** | |
| Management allocates sufficient funds and resources to information security activities. | Yes **No** Don’t  Know |
| Security roles and responsibilities are defined for all staff in the organization. | **Yes** No Don’t  Know |
| The organization’s hiring and termination practices for staff take information security issues into account. | **Yes** No Don’t  Know |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | **Yes** No Don’t  Know |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | **Yes** No Don’t  Know |
| **Security Policies and Regulations** | |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes **No** Don’t  Know |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | **Yes** No Don’t  Know |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | **Yes** No Don’t  Know |
| **Security Policies and Regulations (cont.)** | |
| The organization uniformly enforces its security policies. | **Yes** No Don’t  Know |
| **Collaborative Security Management** | |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | **Yes** No Don’t  Know |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | **Yes** No Don’t  Know |
| **Contingency Planning/Disaster Recovery** | |
| An analysis of operations, applications, and data criticality has been performed. | Yes No **Don’t**  **Know** |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | **Yes** No Don’t  Know |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | **Yes** No Don’t  Know |
| **Contingency Planning/Disaster Recovery (cont.)** | |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | **Yes** No Don’t  Know |
| **Physical Security Plans and Procedures** | |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | **Yes** No Don’t  Know |
| There are documented policies and procedures for managing visitors. | **Yes** No Don’t  Know |
| There are documented policies and procedures for physical control of hardware and software. | **Yes** No Don’t  Know |
| **Physical Access Control** | |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | **Yes** No Don’t  Know |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | **Yes** No Don’t  Know |
| **Monitoring and Auditing Physical Security** | |
| Maintenance records are kept to document the repairs and modifications of a facility’s physical components. | **Yes** No Don’t  Know |
| An individual’s or group’s actions, with respect to all physically controlled media, can be accounted for. | Yes **No** Don’t  Know |
| **Monitoring and Auditing Physical Security (cont.)** | |
| Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed. | **Yes** No Don’t  Know |
| **System and Network Management** | |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | **Yes** No Don’t  Know |
| Sensitive information is protected by secure storage (e.g., backups stored off site, discard process for sensitive information). | **Yes** No Don’t  Know |
| The integrity of installed software is regularly verified. | **Yes** No Don’t  Know |
| All systems are up to date and with respect to revisions, patches, and recommendations in security advisories. | **Yes** No Don’t  Know |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | **Yes** No Don’t  Know |
| Changes to IT hardware and software are planned, controlled, and documented. | **Yes** No Don’t  Know |
| IT staff members follow procedures when issuing, changing, and terminating users’ passwords, accounts, and privileges.   * Unique user identification is required for all information system users, including third-party users. * Default accounts and default passwords have been removed from systems. | **Yes** No Don’t  Know |
| Only necessary services are running on systems – all unnecessary services have been removed. | **Yes** No Don’t  Know |
| **System Administration Tools** | |
| Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. | Yes No **Don’t**  **Know** |
| **Monitoring and Auditing IT Security** | |
| System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure. | **Yes** No Don’t  Know |
| Firewall and other security components are periodically audited for compliance with policy. | **Yes** No Don’t  Know |
| **Authentication and Authorization** | |
| Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections. | **Yes** No Don’t  Know |
| *There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.* | **Yes** No Don’t  Know |
| Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified. | Yes **No** Don’t  Know |
| **Vulnerability Management** | |
| There is a documented set of procedures for managing vulnerabilities, including   * selecting vulnerability evaluation tools, checklists, and scripts * keeping up to date with known vulnerability types and attack methods * reviewing sources of information on vulnerability announcements, security alerts, and notices * identifying infrastructure components to be evaluated * scheduling of vulnerability evaluations * interpreting and responding to the results * maintaining secure storage and disposition of vulnerability data | **Yes** No Don’t  Know |
| Vulnerability management procedures are followed and are periodically reviewed and updated. | Yes **No** Don’t  Know |
| Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified. | Yes **No** Don’t  Know |
| **Encryption** | |
| Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology). | **Yes** No Don’t  Know |
| Encrypted protocols are used when remotely managing systems, routers, and firewalls. | **Yes** No Don’t  Know |
| **Security Architecture and Design** | |
| System architecture and design for new and revised systems include considerations for   * security strategies, policies, and procedures * history of security compromises * results of security risk assessments | **Yes** No Don’t  Know |
| The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology. | **Yes** No Don’t  Know |
| **Incident Management** | |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | **Yes** No Don’t  Know |
| Incident management procedures are periodically tested, verified, and updated. | **Yes** No Don’t  Know |
| There are documented policies and procedures for working with law enforcement agencies. | **Yes** No Don’t  Know |
| **General Staff Practices** | |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | **Yes** No Don’t  Know |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes **No** Don’t  Know |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Yes **No** Don’t  Know |

## Worksheet W3a.5 IT Staff Protection Strategy

| Protection Strategy |
| --- |
| 1. Which issues from the survey would you like to discuss in more detail?  * Monitoring and auditing physical security * Authentication and authorization |
| 1. What important issues did the survey not cover?  * The production staff members are playing on-line games at casino websites on the system terminals. Some of the websites can contain malicious malware that could do serious damage to the production system. * Employee tracking. This is a safety issue as we do not know where people are in the case of an emergency. The scheduling system is our only locator, but not all staff follow them. * The lab needs to have better access control. There are too many unauthorized individuals in the lab. |
| 1. Are there specific security policies, procedures, and practices unique to certain assets? What are they?  * The network is divided into two logical networks: production and administrative. The production network controls the production system and the administrative network provides the production system with data and applications. * The lab is on its own isolated network. |
| 1. Do you think that your organization’s protection strategy is effective?   How do you know?   * Yes – Definitely a lot better then what Swisher had before. There has been almost no incident since I have arrived to this company once I got working on the systems. |

# Process 4

## Worksheet W4.1 Asset Group Worksheet

|  |  |
| --- | --- |
| Asset Group | |
| **Senior Management** | |
| *Important Asset* | *Rationale for Selection* |
| Intellectual Property | Swisher works in a very niche field and they need all the competitive edge they need. Stolen IP can result in loss business to competitors. There is also IP laws in place that Swisher needs to be in compliance with. |
| Client Data | Client information is a critical asset because it can be a breach of a multitude of laws and regulations, depending on the type leaked. One such law is PCI DSS which deals with credit card transactions. |
| Research and Development Data | This is very important as Swisher creates custom products for clients. This data cannot be leaked to the public as their competitors may take it and steal their clients. |

|  |  |
| --- | --- |
| Asset Group | |
| **Operational Area Management** | |
| *Important Asset* | *Rationale for Selection* |
| Production Process/Data | Production is the primary processes that Swisher needs to go through to produce products for their clients. Delays from automated systems could cause loss of future sales. |
| Monitoring System | Safety of staff members as well as general grounds monitoring prevents liabilities for Swisher. The system is on its own network with IoT cameras, as to prevent hackers from jumping from their monitoring system to their primary network. |
| Research and Development Data | This is very important as Swisher creates custom products for clients. This data cannot be leaked to the public as their competitors may take it and steal their clients. Alteration of R&D data could set back productivity by weeks or months as it may have to be reconstructed from scratch. |
| Ordering/Shipping Data | The right materials need to be ordered for products to be produced. The use of wrong materials will produce inferior products, or if delayed, will push back delivery of products to clients by weeks or months. |
| Personnel Data | The primary concern with personnel data is that it keeps its integrity. This includes Personally Identifiable Information, to which should only be available to HR staff. |

|  |  |
| --- | --- |
| Asset Group | |
| **Staff** | |
| *Important Asset* | *Rationale for Selection* |
| Scheduling Data | This is important because it shows the progress of the product and when it is ready for shipment. If the scheduled date is missed, then Swisher could lose a client. The schedule also allows inventory to order materials on time. |
| Inventory Data | Inventory data contains the information that orders the materials to build products for clients. If material isn’t ordered in time, it can set back the delivery date, or in some instances, wrong material may end up being used, creating an inferior product. |
| Production Network | The production network contains all the production computers which have production programs on them. These programs tell the machines what to build, and if correct, then automation takes over. If something is wrong in the production program, then it could waste a bunch of material. |
| IT Administrator | The IT administrator essentially allows the entire company to operate. She ensures the office systems such as computers and other appliances function properly. She also keeps the inventory system working. She also keeps the production network running so automated tasks do not fail. |
| Asset Group | |
| IT Staff | |
| *Important Asset* | *Rationale for Selection* |
| Production System | This allows Swisher to produce products for their clients. This is the primary function of Swisher. |
| Lab System | The lab system contains all the intellectual property and research and development data. This is where all the research is done and tested before being pawned off to the production system for production. |
| Administrative System | The administrative system contains all the intellectual property as alongside the lab system. It also contains the information and data that feeds into the production system alongside the lab system. |
| Network | Broken into two logical networks that run the entirety of Swisher. Production and administration. The production system relies on both logical networks to function, and can only operate for a few hours if one or the other is down. |

### Top Five Critical Assets

|  |  |
| --- | --- |
| **Top 5 Critical Assets** | |
| *Critical Asset* | *Rationale for Selection* |
| Production System | Produces all the products that Swisher sells to clients. Mostly custom built to create the necessary custom products for clients. |
| Scheduling Data | Scheduling data involves everything from staff locations, times, what materials to order for products, as well as how far along the products are in production. |
| Research and Development Data | Swisher creates mostly custom products for clients, and therefore undergo heavy R&D to create those products. Most products require R&D. |
| Inventory System | The inventory system is responsible for having the right materials ready for production. Swisher’s makes custom products for clients, and that requires the proper materials to build. Without the correct material, it puts stress on production machines and creates a suboptimal product. |
| IT Staff | Swisher has gone years hiring a third-party tech support team for their systems, who did not have their best interest. The new IT administrator has gotten the entire system including networks to function properly. |

# Asset Workbooks

## Production System

### Production System Worksheet A4.1 Critical Asset Information

|  |  |
| --- | --- |
| **Critical Asset Information** | |
| Asset | Production System |
| **Rationale for selection as a critical asset** | Produces all the products that Swisher sells to clients. Mostly custom built to create the necessary custom products for clients. |
| **Brief description** | * The production system is responsible for all manufacturing processes. * Contains both Swisher’s and client’s intellectual property * Contains the scheduling system and data * Controls the automation system used for creating products   The production system is one of three parts of Swisher’s IT systems. It contains the scheduling data and controls the production process, which uses automation to build the custom products that Swisher’s clients order. Thus, the system also includes intellectual property, and receives data from both the administrative system and lab system. It is near the final step before delivery of the product, and all other systems and data feeds into it to develop the actual product. |

### Production System Worksheet A4.2 Security Requirements Group Worksheet

| **Security Requirement Type** | **Priority** | **Specific Requirement** |
| --- | --- | --- |
| Confidentiality |  | Intellectual property on the production system needs to be kept confidential at all times as the data on there is subject to the Privacy Act of 1974.  Data on the production system will be restricted on a “need to know” basis. |
| Integrity |  | Process of production and the data being fed to the automation system must be kept accurate to prevent issues from the production process from arising.    Only authorized personnel are allowed to modify data on the system. |
| Availability | X | Access to the production system will be available 24/7. Automated processes for production need to be monitored to prevent issues from arising. |
| Other |  |  |

### Production System Worksheet W4.2 Security Requirements Group Worksheet

| Security Requirements Group | |
| --- | --- |
| Asset: Production System | |
| Security Requirements  (\* indicates most important) | Security Requirements  (\* indicates most important) |
| Senior Management | Operational Area Management |
| AVAILABILITY\*   * System should be available 24/7.   CONFIDENTIALITY\*   * Information on the system should be kept confidential.   INTEGRITY   * Only authorized personnel should have the ability to modify the data. | AVAILABILITY\*   * System should be available 24/7.   CONFIDENTIALITY   * Information on the system should be kept confidential. Subject to a need to know basis.   INTEGRITY   * Only authorized personnel should have the ability to modify the data. |
| Staff | IT Staff |
| AVAILABILITY\*   * System should be available 24/7. Production system controls the automated processes and needs to be monitored when in operation.   CONFIDENTIALITY   * Information on the system should be kept confidential. Subject to a need to know basis.   INTEGRITY\*   * Only authorized personnel should have the ability to modify the data. | AVAILABILITY\*   * System should be available 24/7.   CONFIDENTIALITY   * Information on the system should be kept confidential.   INTEGRITY   * Only authorized personnel should have the ability to modify the data. |

### Production System Worksheet W4.3 Areas of Concern

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Production System** | |
| *Senior Management Area of Concern* | *Impact* |
| (1.1) Afraid of competitors getting a hold of the production system and its processes. | If the way of how Swisher’s runs its production system gets out to our competitors, then we lose our competitive edge.  Access – Network; Physical  Actor – Outsider  Motive – Deliberate  Outcome – Disclosure |
| (1.2) Production system contains the scheduling data, so if it goes down, then shift schedules for production does as well. | The scheduling data is very important as it tells staff members where and when they are supposed to be somewhere. They also give machines instructions on when to operate, as well as the inventory on when to buy materials.  Access – N/A  Actor – System crash; Telecommunications problems or unavailability  Motive – N/A  Outcome – Interruption |
| (1.3) The production system contains all the intellectual property, both Swisher’s and clients. These are data that Swisher would like to keep confidential at all times. | Loss of Swisher’s intellectual property could mean competitors copying what we do. A loss of client intellectual property would be a breach of privacy laws, and their trust.  Access – Network  Actor – Inside  Motive – Accidental  Outcome – Disclosure; Loss, destruction |
| (1.4) Inventory data is also in the production system, and its function is to have information on the correct materials on hand for a specific product being built. | Inventory data keeps the production process running, as it has information on the materials necessary to make a custom product. If materials are not there, then we become delayed in delivering the product to our clients.  Access – Network  Actor – Inside; Telecommunications problems or unavailability  Motive – Accidental  Outcome – Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Production System** | |
| *Operational Area Management Area of Concern* | *Impact* |
| (2.1) Not enough money being spent on production as spent on computers. Need more workers instead of computers controlling the processes. | Production process controlled by automation can mess up, and require troubleshooting by a person. There is only one IT staff but the production process runs all the time. Errors could mean a stop in the production process.  Access – Physical  Actor – Inside  Motive – Accidental  Outcome – Interruption |
| (2.2) Messed up production data from the lab system. | The production process is automated, and gets its schedule and data from the engineers from the system. If it is wrong, then there can be delays as the new production schedule and data needs to be created.  Access – Network; Physical  Actor – Inside  Motive – Accidental  Outcome – Interruption; Loss, destruction |
| (2.3) The production team uses other materials when if they do not have the proper material on hand. | This creates a shortage in materials for other products and may create an inferior final product, which could be faulty or not to our client’s satisfaction.  Access – Physical  Actor – Inside  Motive – Deliberate  Outcome – Modification; Loss, destruction; Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Production System** | |
| *Staff Area of Concern* | *Impact* |
| (3.1) Incorrect data in the production program from the lab. | Having incorrect data would cause the wrong product to be produced, delaying production of the product and destroying material.  Access – N/A  Actor – Software defects  Motive – N/A  Outcome – Loss, destruction; Interruption |
| (3.2) Manager not happy about automated process of the production system. Possible potential for the production manager to voice his opinions and try to get more engineers hired to reduce number of automations on the production floor. | This will cost Swisher more money as it is much more expensive to hire an engineer then have multiple automations run by a few staff.  Access – Physical  Actor – Inside  Motive – Deliberate  Outcome – Modification |
| (3.3) Not being able to monitor and view the production process due to not having the credentials to sign in to a terminal. Only engineers have the credentials to. Production staff need to be ready to update the automated process, but can’t see the status. | This may lead to delays due to not having the knowledge of when a process is over.  Access – Physical  Actor – Inside  Motive – Deliberate  Outcome – Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Production System** | |
| *IT Staff Area of Concern* | *Impact* |
| (4.1) Staff playing games on the production systems could introduce malware into the system if they go on websites laden with that stuff. | Would completely cripple the system, breaching confidentiality and integrity of our data.  Access – N/A  Actor – Virus  Motive – N/A  Outcome – Disclosure; Modification; Loss, destruction; Interruption |
| (4.2) Staff using each other’s IDs and passwords on the production systems. This way, engineers are showing up in many places at once while staff members do not show up at all. | Lack of knowledge of where staff are is a risk in the case of disasters that can cause serious injuries or even death.  Access – Physical  Actor – Inside  Motive – Deliberate  Outcome – Modification; Loss, destruction |
| (4.3) Failure in the production and administrative network which will render the production system capable of running for only a few hours. | Delay in the production processes which will lead to the late delivery of final products.  Access – N/A  Actor – System crashes; Power supply problems  Motive – N/A  Outcome – Loss, destruction; Interruption |

### Production System Worksheet A4.3 Threat Trees

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | (1.3) |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  | (1.3) |
|  |  |  |  |  |  |  |  | interruption |  | (1.4), (2.2) |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
| Production |  | network |  |  |  |  |  |  |  |  |
| System |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | (1.1) |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  | (2.2) |
|  |  |  |  |  |  |  |  | interruption |  | (2.1), (2.2) |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  | (2.3), (3.2)  (4.2) |
|  |  |  |  |  |  |  |  | loss, destruction |  | (2.3), (4.2) |
|  |  |  |  |  |  |  |  | interruption |  | (2.3), (3.3) |
| Production |  | physical |  |  |  |  |  |  |  |  |
| System |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | (1.1) |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

**System Problems**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  | (3.1) |
|  |  |  |  | interruption |  | (3.1) |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  | (4.1) |
|  |  | viruses |  | modification |  | (4.1) |
|  |  |  |  | loss, destruction |  | (4.1) |
|  |  |  |  | interruption |  | (4.1) |
| Production |  |  |  |  |  |  |
| System |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  | (4.3) |
|  |  |  |  | interruption |  | (1.2), (4.3) |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |

**Note**:

**Other Problems**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  | (4.3) |
|  |  |  |  | interruption |  | (4.3) |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | (1.2), (1.4) |
| Production |  |  |  |  |  |  |
| System |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

**Note**:

### Production System Worksheet A5.1 Identify Key Classes of Components

|  |  |
| --- | --- |
| **Production System** | |
| **Class of Component** | **Rationale for Selection** |
| * Servers | Production system information is stored in the company servers. |
| * Networking components | Routers and switches are required to grant internal and access. |
| * Security components | Firewalls in place at routers that connect to the Internet. |
| * Desktop workstations | Used for all production processes. |
| * Home computers |  |
| * Laptops | Sales team needs to produce sales orders as well as estimate R&D expenditure when they need it. |
| * Storage devices | Used to store production system related data. |
| * Wireless components |  |
| * Others (list)   Production floor terminals | Used by production staff and engineer to oversee |

### Production System Worksheet A5.2 Identify Infrastructure Components to Examine

| **Class of Component** | **Selected Component/ IP Addresses/Host Names** | **Rationale** | **Approach** |
| --- | --- | --- | --- |
| System of interest | Production System | The production system is one of the three IT systems that Swisher has and contains many processes and data relating to the production process. | Performance of pass/fail audits on specific components related to the Production System. |
| Systems/servers | Production System Servers | Contain vital processes and instructions related to the production system. | The IT Staff will test the confidentiality and integrity of the production system servers.  1. Verify that all software and programs are up to date.  2. Verify the logs to ensure only authorized personnel have been on the server.  3. Verify that only authorized modifications to the server were made.  4. Verify that only necessary ports are open and vulnerable ones are closed.  5. Verify that there are physical barriers and a door that has a functioning locking mechanism with a pin pad in place.  6. Verify there is a backup schedule. |
| Networking components | Routers and Switches | These devices act as the connection points where data must travel through. | The IT Staff will test whether the routers and switches are configured properly.  1. Verify that the routers are configured to use NAT.  2. Verify that all device connected to the routers and switches are registered.  3. Verify that router log is sent back to the syslog server.  4. Verify that the router has a unique username and password from the default.  5. Verify that all routers and switches are locked behind a physical barrier. |
| Security components | Firewalls | Used to filter incoming and outgoing traffic from the systems to the Internet. | The IT Staff will test that the firewall is properly configured.  1. Verify that the access control list is up to date.  2. Verify that the firewall is sending logs to the syslog server.  3. Verify that the firewall has a unique username and password from the default. |
| Desktop workstations | Staff Workstations | Used by staff members to keep the production system in operation. | The IT Staff will test production staff workstations for possible vulnerabilities.  1. Verify that all staff are using a strong password by running Jack the Ripper on a VM for 24 hours.  2. Verify that there is no software installed on workstations that do not pertain to work.  3. Verify that there are screensavers in place when the workstation is left unattended for 3 minutes.  4. Verify that files with important data are encrypted using VeraCrypt.  5. Verify that workstations do not have keyloggers attached. |
| Home computers | N/A | N/A | N/A |
| Laptops | Sales Team Laptops | Sales team bring laptops to potential and current clients to discuss details of the service. | The IT Staff will test production sales team laptops for possible vulnerabilities.  1. Verify that all staff are using a strong password by running Jack the Ripper on a VM for 24 hours.  2. Verify that there is no software installed on laptops that do not pertain to work.  3. Verify that there are screensavers in place when the laptop is left unattended for 3 minutes.  4. Verify that files with important data are encrypted using VeraCrypt.  5. Verify that all laptops are using a VPN service. |
| Storage devices | Network Attached Storage | Contain vital data related to IP, scheduling, processes, inventory, and sales. | The IT Staff will test the network attached storage for vulnerabilities and ensure that it is able to keep data confidential and available.  1. Verify that the NAS software is up to date.  2. Verify that the default administrator account is disabled.  3. Verify there is a firewall in place.  4. Verify that all NAS are locked behind a physical barrier.  5. Verify there is a backup schedule. |
| Wireless components | N/A | N/A | N/A |
| Others | Production Floor Terminals | Used by production staff and engineers to oversee the status of the machines. | The IT Staff will test the production floor terminals for vulnerabilities.  1. Verify that the terminal software is up to date.  2. Verify that there is no software downloaded on the terminals not pertaining to work.  3. Verify that there is an antivirus installed on the terminals. |

### Production System Worksheet A6.1 Review Technology Vulnerabilities and Summarize Results

| **Asset: Production System** | | | |
| --- | --- | --- | --- |
| **Class** | **Selected Component/ IP Address/Host Name** | **Results** | **Vulnerability Summary** |
| System/  servers | Production System Servers | 1. Fail  2. Fail  3. Fail  4. Pass  5. Pass  6. Fail | - medium  - high  - medium  - low |
| Networking  components | Routers and Switches | 1. Pass  2. Fail  3. Pass  4. Pass  5. Fail | - low  - low |
| Security  components | Firewalls | 1. Fail  2. Pass  3. Pass | - medium |
| Desktop  workstations | Staff Workstations | 1. Fail  2. Fail  3. Fail  4. Fail  5. Fail | - medium  - low  - medium  - medium  - high |
| Laptops | Sales Team Laptops | 1. Fail  2. Pass  3. Fail  4. Fail  5. Pass | - medium  - medium  - medium |
| Storage  devices | Network Attached Storage | 1. Fail  2. Pass  3. Fail  4. Fail  5. Pass | - medium  - low  - low |
| Others | Production Floor Terminals | 1. Fail  2. Fail  3. Fail | - medium  - low  - medium |

|  |
| --- |
| **Actions and Recommendations for Addressing Technology Vulnerabilities** |
| **Company-wide Vulnerabilities** |
| Routers and Switches – The devices that connect to the router and switches are not all registered. Unregistered devices may not belong to staff, which can pose serious risks as the individual is now within Swisher’s network. The other vulnerability is physical, in the fact that the routers and switches are not locked away in a physical container/barrier of sorts. Both of these vulnerabilities are of low severity and can be fixed at a later day. |
| Firewalls – The firewalls are assigned to the production and inventory systems. The only vulnerability is of medium severity, and that is because the access control list is not up to date. This can allow unwanted data packets from entering the network and the systems. |
| Network Attached Storage – NAS is used across the network, but the lab system that holds the R&D data have a separate one. There is one medium and two low severities. The medium is the NAS software is not up to date. Update contain various security patches that keep the NAS device from known vulnerabilities. The two lows are that there is no firewall in place, and there is no physical barrier protecting the NAS. Firewalls help protect the data on the NAS device by filtering traffic in and out. No physical barriers could mean someone could gain access to the NAS device rather easily. |

|  |
| --- |
| **Actions and Recommendations for Addressing Technology Vulnerabilities** |
| **Production System Vulnerabilities** |
| Production System Servers – There is one high, two medium, and one low severity vulnerabilities. The high severity is that there are unauthorized personnel on the server, which could lead to many issues such as confidentiality of data, integrity of data, as well as availability of the server. The two medium severity issues are that the software on the server is not update and non-authorized modifications were made on the server. The latest software updates usually contain security patches to protect against known vulnerabilities in the software. Non-authorized modifications can lead to an integrity and availability issue. The low severity issue is that there are no backups scheduled for the server. Though preferable, the lack of a backup is not an immediate threat to Swisher. A backup is recommended, however, as system crashes or incidents where data is lost may occur. |
| Staff Workstations – The staff workstations contained one high, three mediums, and one low severity. The high severity issue is that a keylogger was discovered on one of the workstations. Keyloggers are usually put on computers to steal passwords, which can grant immediate access to the workstation. The recommendation is for staff to always check what peripherals are connected to their workstations before proceeding to use it. The three medium severity issues are that the staff use weak passwords, do not have screensavers that meet a 3-minute requirement, and that confidential data is not being encrypted with VeraCrypt. Weak passwords are easy to compromise, and thus a password policy should be created. Screensavers help protect the information on a workstation if one forgets to lock their screen, otherwise, others can use the workstation in its current session. Confidential information should always require a form of encryption to add additional layers of security in case it gets compromised. The low severity issue pertains with unnecessary software on the workstation. This software could possibly have malicious content on them. It is best to not download anything that doesn’t pertain to work on workstations at Swisher. |
| Sales Team Laptops – The sales team laptops have three medium severity issues. The three issues are that the sales team use weak passwords, do not have screensavers that meet a 3-minute requirement, and that confidential data is not being encrypted with VeraCrypt. Weak passwords are easy to compromise, and thus a password policy should be created. Screensavers help protect the information on a laptop if one forgets to lock their screen, otherwise, others can use the laptop in its current session. Confidential information should always require a form of encryption to add additional layers of security in case it gets compromised. |
| Production Floor Terminals – The production floor terminals contain two medium and one low severity issue. The two medium severity issues are that the terminal software is not up to date and there is no antivirus software installed on the terminals. The latest software updates usually contain security patches to protect against known vulnerabilities in the software. Antivirus software should be used, and in this case, because production staff play online games on websites that may contain malware. The low severity issue pertains with unnecessary software on the terminals. This software could possibly have malicious content on them. It is best to not download anything that doesn’t pertain to work on workstations at Swisher. |

### Production System Worksheet A7.1 Identify the Impact of Threats to Critical Assets

| **Production System** | | | |
| --- | --- | --- | --- |
| **Impacts to the Organization** | | | |
| **Outcome** | **Consider** | **Impact Descriptions** | **Values** |
| **Disclosure** | * How could the organization’s reputation be affected if this asset were disclosed? * How could customer confidence be affected if this asset were disclosed? * How could the health of customers be affected if this asset were disclosed? * How could employee productivity be affected if this asset were disclosed? * How would other users of this asset be affected if this asset were disclosed? * What fines, legal penalties, or lawsuits could be imposed as a result of disclosure of this asset? * How could the organization be affected financially if this asset were disclosed? * What other impacts could occur if this asset were disclosed? For example: * ethical considerations * other legal/financial impacts | * The production system contains much information relating to the production process, as well as intellectual property, Swisher’s and clients. If client IP were to be leaked, trust in Swisher’s ability to secure data would impact their business. * Customer confidence would drop significantly if the production system were disclosed because it means that Swisher does not have the means to protect their information assets. * Disclosure of the production system has no ill effect on customer’s health. * Disclosure of the production system may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the production system more secure. * Users of the production system would not be affected as disclosure means that the information was leaked/taken. It does not change the integrity of the production system. * Disclosure of the production system would mean possible disclosure of customer IP. This would be a breach in consumer data privacy laws such as the GDPR for European customers and the US Privacy Act of 1974 for US customers. * Disclosure of the production system would mean losing the competitive edge Swisher has in the market due to their production processes. This could result in a loss of customers attracted to competitors. * All considerations to disclosure of impacts have been made in relation to Swisher’s production system. |  |
| **Modification** | * How could the organization’s reputation be affected if this asset were modified? * How could customer confidence be affected if this asset were modified? * How could the health of customers be affected if this asset were modified? * How could employee productivity be affected if this asset were modified? * How would other users of this asset be affected if this asset were modified? * What fines, legal penalties, or lawsuits could be imposed as a result of modification of this asset? * How could the organization be affected financially if this asset were modified? * What other impacts could occur if this asset were modified? For example: * ethical considerations * other legal/financial impacts | * Modification of the production system would affect the reputation of Swisher depending on the modification actor. The production system contains much information relating to the production process, as well as intellectual property, Swisher’s and clients. If client IP were to be modified by an external actor, trust in Swisher’s ability to secure data would impact their business. * Customer confidence would drop significantly if the production system were modified because it means that Swisher does not have the means to protect their information assets. * Modification of the production system has no ill effect on customer health. * Modification of the production system may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the production system more secure. * There are no other users of the production system other than the staff at Swisher. * Modification of the production system would mean possible modification of customer IP. This would be a breach in consumer data privacy laws such as the GDPR for European customers and the US Privacy Act of 1974 for US customers. * Modification of the production system would mean losing the competitive edge Swisher has in the market due to their production processes. This could result in a loss of customers attracted to competitors. * All considerations to modification of impacts have been made in relation to Swisher’s production system. |  |
| **Destruction/Loss** | * How could the organization’s reputation be affected if this asset were destroyed, lost, or unavailable? * How could customer confidence be affected if this asset were destroyed, lost, or unavailable? * How could the health of customers be affected if this asset were destroyed, lost, or unavailable? * How could employee productivity be affected if this asset were destroyed, lost, or unavailable? * How would other users of this asset be affected if this asset were destroyed, lost, or unavailable? * What fines, legal penalties, or lawsuits could be imposed as a result of destruction/loss of this asset? * How could the organization be affected financially if this asset were destroyed, lost, or unavailable? * What other impacts could occur if this asset were destroyed, lost, or unavailable? For example: * ethical considerations * other legal/financial impacts | * The production system contains much information relating to the production process, as well as intellectual property, Swisher’s and clients. If client IP were to be destroyed/lost, trust in Swisher’s ability to secure data would impact their business. * Customer confidence would drop significantly if the production system were destroyed/lost because it means that Swisher does not have the means to protect their information assets. * Destruction/loss of the production system has no ill effect on customer’s health. * Destruction/loss of the production system may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the production system more secure. * There are no other users of the production system other than the staff at Swisher. * Destruction/loss of the production system at Swisher’s does not breach any laws or regulations and not subject to legal penalties. * Destruction/loss of the production system would mean losing the competitive edge Swisher has in the market due to their production processes. This could result in a loss of customers attracted to competitors. * All considerations to destruction/loss of impacts have been made in relation to Swisher’s production system. |  |
| **Interruption** | * How could the organization’s reputation be affected if access to this asset were unavailable? * How could customer confidence be affected if access to this asset were unavailable? * How could the health of customers be affected if access to this asset were unavailable? * How could employee productivity be affected if access to this asset were unavailable? * How would other users of this asset be affected if access to this asset were unavailable? * What fines, legal penalties, or lawsuits could be imposed as a result of unavailability of this asset? * How could the organization be affected financially if access to this asset were unavailable? * What other impacts could occur if access to this asset were unavailable? For example: * ethical considerations * other legal/financial impacts | * The production system contains much information relating to the production process, as well as intellectual property, Swisher’s and clients. If client IP were to be unavailable, trust in Swisher’s ability to secure data would impact their business. * Customer confidence would drop significantly if the production system were unavailable because it means that Swisher does not have the means to protect their information assets. * Unavailability of the production system has no ill effect on customer’s health. * Unavailability of the production system may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the production system more secure. * There are no other users of the production system other than the staff at Swisher. * Unavailability of the production system at Swisher’s does not breach any laws or regulations and not subject to legal penalties. * Unavailability of the production system would mean losing the competitive edge Swisher has in the market due to their production processes. This could result in a loss of customers attracted to competitors. * All considerations to unavailability of impacts have been made in relation to Swisher’s production system. |  |

### Production System Worksheet A7.2 Create Risk Evaluation Criteria

| Production System Evaluation Criteria | | | |
| --- | --- | --- | --- |
| **Impact Area** | **High** | **Medium** | **Low** |
| Reputation/ Customer Confidence | * Reputation irrevocably destroyed or damaged * More than 30% drop in customers due to loss of confidence | * Reputation damaged; some effort and expense required to recover * 10 to 30% drop in customers due to loss of confidence * Customer goes to competitor | * Reputation minimally affected; little or no effort or expense required to recover * Less than 10% drop in customers due to loss of confidence |
| Life/ Health of Customers | * Loss of customer life * Permanent impairment of one or more significant aspects of customer’s health (e.g., loss of use of one or more limbs, blindness, brain damage) * Safety violated | * Customer life threatened but recoverable with additional treatment * Temporary or recoverable impairment of customer’s health (e.g., recovering use of limbs through physical therapy) * Safety affected | * No loss or significant threat to customer life * Minimal, immediately treatable degradation in customer heath with recovery within four days * Safety questioned |
| Productivity | * Staff unable to perform critical job aspects for three or more days * 40% or more increase in work hours required of at least 10% of general staff for > three days * Irrecoverable loss of server data | * Staff work increased by 10-40% for one day * Increases in general staff work of 10-40% for one day * Inefficient continuity of availability; delays while recovering misplaced information | * Staff inconvenienced for less than a day but no measurable increase in work effort occurs * General staff inconvenienced for less than a day but no measurable increase in work effort occurs |
| Fines/ Legal Penalties | * Fines of greater than $100,000 levied * One or more non-frivolous lawsuits of more than $3,000,000 filed by customers * Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices | * Fines of $10,000 to $100,000 levied * One or more non-frivolous lawsuits between $250,000 and $3,000,000 filed by customers * Government or other investigative organization requests information or records (low-profile) | * No fine or a fine of less than $10,000 levied * Lawsuit of less than $250,000 or frivolous lawsuit (95% sure it can be defeated) filed by customer * No queries from government or other investigative organizations |
| Finances | * Yearly operational costs up 15% * 20% yearly revenue loss * One-time financial cost > $1M * Uncorrectable errors in funding and personnel | * Yearly operational costs up 2-15% * 5-20% yearly revenue loss * One-time financial cost of $25K to $1M * Partially correctable errors in funding and personnel | * Increase of less than 2% in operating costs * <5% yearly revenue loss * One-time financial cost of <$25K * Inconvenient but correctable errors in funding and personnel |

### Production System Worksheet A7.3 Evaluate the Impacts of Threats to Critical Assets

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Medium |
|  |  |  |  |  |  | accidental |  | modification |  | Medium |
|  |  |  |  |  |  |  |  | loss, destruction |  | High |
|  |  |  |  |  |  |  |  | interruption |  | Low |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Medium |
|  |  |  |  |  |  | deliberate |  | modification |  | Medium |
|  |  |  |  |  |  |  |  | loss, destruction |  | High |
|  |  |  |  |  |  |  |  | interruption |  | Low |
| Production |  | network |  |  |  |  |  |  |  |  |
| System |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Medium |
|  |  |  |  |  |  | deliberate |  | modification |  | Medium |
|  |  |  |  |  |  |  |  | loss, destruction |  | High |
|  |  |  |  |  |  |  |  | interruption |  | Low |

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  | |  |  |  |  | |
|  |  |  |  |  |  |  | |  | disclosure |  |  | |
|  |  |  |  |  |  | accidental | |  | modification |  |  | |
|  |  |  |  |  |  |  | |  | loss, destruction |  | High | |
|  |  |  |  |  |  |  | |  | interruption |  | Low | |
|  |  |  |  | inside |  |  | |  |  |  |  | |
|  |  |  |  |  |  |  | |  | disclosure |  |  | |
|  |  |  |  |  |  | deliberate | |  | modification |  | Medium | |
|  |  |  |  |  |  |  | |  | loss, destruction |  | High | |
|  |  |  |  |  |  |  | |  | interruption |  | Low | |
| Production |  | physical |  |  |  |  | |  |  |  |  | |
| System |  |  |  |  |  |  | |  | disclosure |  |  | |
|  |  |  |  |  |  | accidental | |  | modification |  |  | |
|  |  |  |  |  |  |  | |  | loss, destruction |  |  | |
|  |  |  |  |  |  |  | |  | interruption |  |  | |
|  |  |  |  | outside |  |  | |  |  |  |  | |
|  |  |  |  |  |  |  | |  | disclosure |  | High | |
|  |  |  |  |  |  | deliberate | |  | modification |  |  | |
|  |  |  |  |  |  |  | |  | loss, destruction |  |  | |
|  |  |  |  |  |  |  | |  | interruption |  |  | |

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  | High |
|  |  |  |  | interruption |  | Low |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  | Medium |
|  |  | viruses |  | modification |  | Medium |
|  |  |  |  | loss, destruction |  | High |
|  |  |  |  | interruption |  | Low |
| Production |  |  |  |  |  |  |
| System |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  | High |
|  |  |  |  | interruption |  | Low |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  | High |
|  |  |  |  | interruption |  | Low |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | Low |
| Production |  |  |  |  |  |  |
| System |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

## Scheduling Data

### Scheduling Data Worksheet A4.1 Critical Asset Information

|  |  |
| --- | --- |
| **Critical Asset Information** | |
| Asset | Scheduling Data |
| **Rationale for selection as a critical asset** | Scheduling data involves everything from staff locations, times, what materials to order for products, as well as how far along the products are in production. |
| **Brief description** | * Part of the production system. * Contains schedule information for both humans and machines   The scheduling data is found inside the production system, which is one of the critical assets as well. Found inside the scheduling system, all human and machine schedules are listed. For humans, it lists where staff should be during what times during the day. For machines, it tells them when to begin tasks such as the automated production systems. The scheduling system is also tasked with sending out data to the inventory systems which will put in orders for new products that are scheduled to be made. This in turn, affects accounting as placed orders need to be updated in the books. |

### Scheduling Data Worksheet A4.2 Security Requirements Group Worksheet

| **Security Requirement Type** | **Priority** | **Specific Requirement** |
| --- | --- | --- |
| Confidentiality |  | Intellectual property on the production system needs to be kept confidential at all times.  Scheduling data will be restricted on a “need to know” basis. |
| Integrity |  | Scheduling data must be kept accurate at all times and respective information should be available to all staff members at all times.  Only authorized personnel are allowed to modify the scheduling data. |
| Availability | X | Access to the scheduling data will be available 24/7.  This allows staff members to see where they need to be during the day as well as for the machines to update other systems. |
| Other |  |  |

### Scheduling Data Worksheet W4.2 Security Requirements Group Worksheet

| Security Requirements Group | |
| --- | --- |
| Asset: Scheduling Data | |
| Security Requirements  (\* indicates most important) | Security Requirements  (\* indicates most important) |
| Senior Management | Operational Area Management |
| AVAILABILITY\*   * Scheduling data should be available 24/7.   CONFIDENTIALITY   * Scheduling data should be kept confidential at all times. Subject to a need to know basis.   INTEGRITY\*   * Scheduling data can only be modified by authorized personnel. | AVAILABILITY\*   * Scheduling data should be available 24/7.   CONFIDENTIALITY   * Scheduling data should be kept confidential at all times. Subject to a need to know basis.   INTEGRITY\*   * Scheduling data can only be modified by authorized personnel. |
| Staff | IT Staff |
| AVAILABILITY\*   * Scheduling data should be available 24/7.   CONFIDENTIALITY\*   * Scheduling data should be kept confidential at all times. Subject to a need to know basis.   INTEGRITY\*   * Scheduling data can only be modified by authorized personnel. | AVAILABILITY\*   * Scheduling data should be available 24/7.   CONFIDENTIALITY   * Scheduling data should be kept confidential at all times. Subject to a need to know basis.   INTEGRITY\*   * Scheduling data can only be modified by authorized personnel. |

### Scheduling Data Worksheet W4.3 Areas of Concern

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset:** **Scheduling Data** | |
| *Senior Management Area of Concern* | *Impact* |
| (1.1) The integrity of the scheduling data must be unmodified and accurate. | If scheduling data is wrong, then people end up in places that they are not supposed to be and production gets delayed.  Access – Network; Physical  Actor – Inside  Motive – Accidental  Outcome – Modification; Interruption |
| (1.2) Snowballing effect from a single schedule error. | When scheduling data is incorrect, then we get production backups, where it gets held up due to a schedule error. Missing sales goals loses Swisher money.  Access – Network  Actor – Inside  Motive – Accidental  Outcome – Loss, destruction |
| (1.3) Snowballing effect from a single schedule error. Delay of products to clients. | Once a single product is held up, then the next product gets held up as well, as the first one needs to be fixed. This puts stress on our relationships with clients if they do not get their products on time.  Access – Network  Actor – Inside  Motive – Accidental  Outcome – Loss, destruction; Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Scheduling Data** | |
| *Operational Area Management Area of Concern* | *Impact* |
| (2.1) Production scheduling being messed up, preventing the production process from beginning or continuing. | We end up delaying our production and final product to our clients.  Access – N/A  Actor – Software defects  Motive – N/A  Outcome – Interruption |
| (2.2) Safety of staff members if the scheduling data is not being followed or incorrect. Scheduling data has information on where and when staff are supposed to be at a location. | People can die or be badly hurt if we do not know their location in the event of a disaster.  Access – N/A  Actor – Telecommunications problems or unavailability  Motive – N/A  Outcome – Loss, destruction; Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Scheduling Data** | |
| *Staff Area of Concern* | *Impact* |
| (3.1) That the scheduling system becomes unavailable so we will not be able to see the progress of the products. We build custom products for our clients and many want to see the progress we’ve made, which is stored in the scheduling system. | Cannot provide data to clients when they request it.  Access – N/A  Actor – Software defects  Motive – N/A  Outcome – Interruption |
| (3.2) Inaccuracy of the scheduling data related to orders. The scheduling system alerts staff to what is being produced and affects their ordering of material. | Storage of expensive materials on-site, which can be stolen. Payment of premium shipping at Swisher’s expense.  Access – Network  Actor – Inside  Motive – Accidental  Outcome – Modification; Loss, destruction; Interruption |
| (3.3) Integrity of the scheduling information in relation to the production process. Scheduling information tells the staff on what materials to pick up from inventory and tells the automated machines how to create the product. | Having incorrect data would cause the wrong product to be produced, delaying production of the product and destroying material.  Access – Physical  Actor – Inside  Motive – Accidental  Outcome –Modification; Loss, destruction; Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Scheduling Data** | |
| *IT Staff Area of Concern* | *Impact* |
| (4.1) Not knowing where the staff are as they are scheduled to be. They use each other’s IDs and passwords, so they are never in the right locations that they are scheduled to be in the system. | Lack of knowledge of where staff members are is a risk in the case of disasters that can cause serious injuries or even death.  Access – Physical  Actor – Inside  Motive – Deliberate  Outcome – Loss, destruction; Interruption |

### Scheduling Data Worksheet A4.3 Threat Trees

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  | (1.1), (3.2) |
|  |  |  |  |  |  |  |  | loss, destruction |  | (1.2), (1.3)  (3.2) |
|  |  |  |  |  |  |  |  | interruption |  | (1.1), (1.3)  (3.2) |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
| Scheduling |  | network |  |  |  |  |  |  |  |  |
| Data |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  | (1.1), (3.3) |
|  |  |  |  |  |  |  |  | loss, destruction |  | (3.3) |
|  |  |  |  |  |  |  |  | interruption |  | (1.1), (3.3) |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  | (4.1) |
|  |  |  |  |  |  |  |  | interruption |  | (4.1) |
| Scheduling |  | physical |  |  |  |  |  |  |  |  |
| Data |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

* (4.1) Concerned with loss of life due to employees not following schedule data.

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | (2.1), (3.1) |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | viruses |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
| Scheduling |  |  |  |  |  |  |
| Data |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |

**Note**:

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  | (2.2) |
|  |  |  |  | interruption |  | (2.2) |
| Scheduling |  |  |  |  |  |  |
| Data |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

**Note**:

* (2.2) Concerned with injury or loss of life due to disasters in the case of an unavailable schedule, disabling the location identifiability of employees.

### Scheduling Data Worksheet A5.1 Identify Key Classes of Components

|  |  |
| --- | --- |
| **Scheduling Data** | |
| **Class of Component** | **Rationale for Selection** |
| * Servers | Scheduling data is stored in the production servers. |
| * Networking components | Routers and switches are required to grant internal and access. |
| * Security components | Encryption standards in place to ensure confidentiality and integrity of the data. |
| * Desktop workstations | Staff workstations used to update and maintain the scheduling data. |
| * Home computers |  |
| * Laptops |  |
| * Storage devices | Used to store scheduling data. |
| * Wireless components |  |
| * Others (list)   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

### Scheduling Data Worksheet A5.2 Identify Infrastructure Components to Examine

| **Class of Component** | **Selected Component/ IP Addresses/Host Names** | **Rationale** | **Approach** |
| --- | --- | --- | --- |
| System of interest | Scheduling Data | The scheduling data contains human and machine schedules. | Performance of pass/fail audits on specific components related to Scheduling Data. |
| Systems/servers | Production System Servers | Contain vital processes and instructions related to scheduling data. | Performed in conjunction with production system\* |
| Networking components | Routers and Switches | These devices act as the connection points where data must travel through. | Performed in conjunction with production system\* |
| Security components | Encryption Methods | Scheduling data should be kept confidential, and an encryption method would be the best way to do that. | The IT Staff will test whether the scheduling data is properly encrypted or not.  1. Verify that VeraCrypt is installed on the workstations that have inventory data on it.  2. Verify that all files with scheduling data are encrypted with VeraCrypt.  3. Verify that authorized staff who use the inventory workstations to modify inventory data are using VeraCrypt properly. |
| Desktop workstations | Staff Workstations | Scheduling data will be available on specific workstations that allow authorized staff to place and update orders. | The IT Staff will test scheduling workstations for possible vulnerabilities.  1. Verify that all staff are using a strong password by running Jack the Ripper on a VM for 24 hours.  2. Verify that there is no software installed on workstations that do not pertain to work.  3. Verify that there are screensavers in place when the workstation is left unattended for 3 minutes.  4. Verify that files with important data are encrypted using VeraCrypt.  5. Verify that workstations do not have keyloggers attached. |
| Home computers | N/A | N/A | N/A |
| Laptops | N/A | N/A | N/A |
| Storage devices | Network Attached Storage | Used to store scheduling data. | Performed in conjunction with production system\* |
| Wireless components | N/A | N/A | N/A |
| Others | N/A | N/A | N/A |

### Scheduling Data Worksheet A6.1 Review Technology Vulnerabilities and Summarize Results

| **Asset: Scheduling Data** | | | |
| --- | --- | --- | --- |
| **Class** | **Selected Component/ IP Address/Host Name** | **Results** | **Vulnerability Summary** |
| Systems/  servers | Production System Servers | Performed in conjunction with production system\* | Performed in conjunction with production system\* |
| Networking  components | Routers and Switches | 1. Pass  2. Fail  3. Pass  4. Pass  5. Fail | - low  - low |
| Security  components | Encryption Methods | 1. Fail  2. Fail  3. Fail | - medium  - medium  - medium |
| Desktop  workstations | Staff Workstations | 1. Fail  2. Fail  3. Fail  4. Fail  5. Pass | - medium  - low  - medium  - medium |
| Storage  devices | Network Attached Storage | 1. Fail  2. Pass  3. Fail  4. Fail  5. Pass | - medium  - low  - low |

|  |
| --- |
| **Actions and Recommendations for Addressing Technology Vulnerabilities** |
| **Company-wide Vulnerabilities** |
| Routers and Switches – The devices that connect to the router and switches are not all registered. Unregistered devices may not belong to staff, which can pose serious risks as the individual is now within Swisher’s network. The other vulnerability is physical, in the fact that the routers and switches are not locked away in a physical container/barrier of sorts. Both of these vulnerabilities are of low severity and can be fixed at a later day. |
| Firewalls – The firewalls are assigned to the production and inventory systems. The only vulnerability is of medium severity, and that is because the access control list is not up to date. This can allow unwanted data packets from entering the network and the systems. |
| Network Attached Storage – NAS is used across the network, but the lab system that holds the R&D data have a separate one. There is one medium and two low severities. The medium is the NAS software is not up to date. Update contain various security patches that keep the NAS device from known vulnerabilities. The two lows are that there is no firewall in place, and there is no physical barrier protecting the NAS. Firewalls help protect the data on the NAS device by filtering traffic in and out. No physical barriers could mean someone could gain access to the NAS device rather easily. |

|  |
| --- |
| **Actions and Recommendations for Addressing Technology Vulnerabilities** |
| **Scheduling Data Vulnerabilities** |
| Encryption Methods – The encryption method for the scheduling data contains three medium severity issues. VeraCrypt is not installed on any of the workstations that contain scheduling or R&D data. This is a vulnerability as the data can easily be read as there is no encryption on them. This fails the other two audits immediately, as none of the files are encrypted, and we cannot test whether the staff have been using VeraCrypt properly, as it is not even downloaded. |
| Staff Workstation – The scheduling staff workstations have three medium and one low severity issues. The three medium severity issues are that the staff use weak passwords, do not have screensavers that meet a 3-minute requirement, and that confidential data is not being encrypted with VeraCrypt. Weak passwords are easy to compromise, and thus a password policy should be created. Screensavers help protect the information on a workstation if one forgets to lock their screen, otherwise, others can use the workstation in its current session. Confidential information should always require a form of encryption to add additional layers of security in case it gets compromised. The low severity issue pertains with unnecessary software on the workstation. |

### Scheduling Data Worksheet A7.1 Identify the Impact of Threats to Critical Assets

| **Scheduling Data** | | | |
| --- | --- | --- | --- |
| **Impacts to the Organization** | | | |
| **Outcome** | **Consider** | **Impact Descriptions** | **Values** |
| **Disclosure** | * How could the organization’s reputation be affected if this asset were disclosed? * How could customer confidence be affected if this asset were disclosed? * How could the health of customers be affected if this asset were disclosed? * How could employee productivity be affected if this asset were disclosed? * How would other users of this asset be affected if this asset were disclosed? * What fines, legal penalties, or lawsuits could be imposed as a result of disclosure of this asset? * How could the organization be affected financially if this asset were disclosed? * What other impacts could occur if this asset were disclosed? For example: * ethical considerations * other legal/financial impacts | * If scheduling data were to be disclosed, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the scheduling data were disclosed because it means that Swisher does not have the means to protect their information assets. * Disclosure of the scheduling data has no ill effect on customer’s health. * Disclosure of the scheduling data may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the scheduling data more secure. * Users of the scheduling data would not be affected as disclosure means that the information was leaked/taken. It does not change the integrity of the scheduling data. * Disclosure of the scheduling data would mean possible disclosure of customer and vendor information. This would be a breach in consumer data privacy laws such as the GDPR for European customers and the US Privacy Act of 1974 for US customers. * Disclosure of the scheduling data has little financial affect for Swisher. * All considerations to disclosure of impacts have been made in relation to Swisher’s scheduling data. |  |
| **Modification** | * How could the organization’s reputation be affected if this asset were modified? * How could customer confidence be affected if this asset were modified? * How could the health of customers be affected if this asset were modified? * How could employee productivity be affected if this asset were modified? * How would other users of this asset be affected if this asset were modified? * What fines, legal penalties, or lawsuits could be imposed as a result of modification of this asset? * How could the organization be affected financially if this asset were modified? * What other impacts could occur if this asset were modified? For example: * ethical considerations * other legal/financial impacts | * If scheduling data were to be modified, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect the integrity of their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the production system were disclosed because it means that Swisher does not have the means to protect their information assets. * Modification of the scheduling data has no ill effect on customer health. * Disclosure of the scheduling data may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the scheduling data more secure. * There are no other users of the scheduling data other than the staff at Swisher. * Modification of the scheduling data would mean possible modification of customer and vendor information. This would be a breach in consumer data privacy laws such as the GDPR for European customers and the US Privacy Act of 1974 for US customers. * Modification of the scheduling data has little financial affect for Swisher. * All considerations to modification of impacts have been made in relation to Swisher’s scheduling data. |  |
| **Destruction/Loss** | * How could the organization’s reputation be affected if this asset were destroyed, lost, or unavailable? * How could customer confidence be affected if this asset were destroyed, lost, or unavailable? * How could the health of customers be affected if this asset were destroyed, lost, or unavailable? * How could employee productivity be affected if this asset were destroyed, lost, or unavailable? * How would other users of this asset be affected if this asset were destroyed, lost, or unavailable? * What fines, legal penalties, or lawsuits could be imposed as a result of destruction/loss of this asset? * How could the organization be affected financially if this asset were destroyed, lost, or unavailable? * What other impacts could occur if this asset were destroyed, lost, or unavailable? For example: * ethical considerations * other legal/financial impacts | * If scheduling data were to be destroyed/lost, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the scheduling data were destroyed/lost because it means that Swisher does not have the means to protect their information assets. * Destruction/loss of the scheduling data has no ill effect on customer’s health. * Destruction/loss of the scheduling data may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the scheduling data more secure. * There are no other users of the scheduling data other than the staff at Swisher. * Destruction/loss of the scheduling data at Swisher’s does not breach any laws or regulations and not subject to legal penalties. * Destruction/loss of the scheduling data would mean losing the competitive edge Swisher has in the market due to their production processes. This could result in a loss of customers attracted to competitors. * All considerations to destruction/loss of impacts have been made in relation to Swisher’s scheduling data. |  |
| **Interruption** | * How could the organization’s reputation be affected if access to this asset were unavailable? * How could customer confidence be affected if access to this asset were unavailable? * How could the health of customers be affected if access to this asset were unavailable? * How could employee productivity be affected if access to this asset were unavailable? * How would other users of this asset be affected if access to this asset were unavailable? * What fines, legal penalties, or lawsuits could be imposed as a result of unavailability of this asset? * How could the organization be affected financially if access to this asset were unavailable? * What other impacts could occur if access to this asset were unavailable? For example: * ethical considerations * other legal/financial impacts | * If scheduling data were to be unavailable, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the scheduling data were unavailable because it means that Swisher does not have the means to protect their information assets. * Unavailability of the scheduling data has no ill effect on customer’s health. * Unavailability of the scheduling data may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the scheduling data more secure. * There are no other users of the scheduling data other than the staff at Swisher. * Unavailability of the scheduling data at Swisher’s does not breach any laws or regulations and not subject to legal penalties. * Unavailability of the scheduling data would mean losing the competitive edge Swisher has in the market due to their production processes. This could result in a loss of customers attracted to competitors. * All considerations to unavailability of impacts have been made in relation to Swisher’s scheduling data. |  |

### Scheduling Data Worksheet A7.2 Create Risk Evaluation Criteria

| Scheduling Data Evaluation Criteria | | | |
| --- | --- | --- | --- |
| **Impact Area** | **High** | **Medium** | **Low** |
| Reputation/ Customer Confidence | * Reputation irrevocably destroyed or damaged * More than 30% drop in customers due to loss of confidence | * Reputation damaged; some effort and expense required to recover * 10 to 30% drop in customers due to loss of confidence * Customer goes to competitor | * Reputation minimally affected; little or no effort or expense required to recover * Less than 10% drop in customers due to loss of confidence |
| Life/ Health of Customers | * Loss of customer life * Permanent impairment of one or more significant aspects of customer’s health (e.g., loss of use of one or more limbs, blindness, brain damage) * Safety violated | * Customer life threatened but recoverable with additional treatment * Temporary or recoverable impairment of customer’s health (e.g., recovering use of limbs through physical therapy) * Safety affected | * No loss or significant threat to customer life * Minimal, immediately treatable degradation in customer heath with recovery within four days * Safety questioned |
| Productivity | * Staff unable to perform critical job aspects for three or more days * 40% or more increase in work hours required of at least 10% of general staff for > three days * Irrecoverable loss of server data | * Staff work increased by 10-40% for one day * Increases in general staff work of 10-40% for one day * Inefficient continuity of availability; delays while recovering misplaced information | * Staff inconvenienced for less than a day but no measurable increase in work effort occurs * General staff inconvenienced for less than a day but no measurable increase in work effort occurs |
| Fines/ Legal Penalties | * Fines of greater than $100,000 levied * One or more non-frivolous lawsuits of more than $3,000,000 filed by customers * Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices | * Fines of $10,000 to $100,000 levied * One or more non-frivolous lawsuits between $250,000 and $3,000,000 filed by customers * Government or other investigative organization requests information or records (low-profile) | * No fine or a fine of less than $10,000 levied * Lawsuit of less than $250,000 or frivolous lawsuit (95% sure it can be defeated) filed by customer * No queries from government or other investigative organizations |
| Finances | * Yearly operational costs up 15% * 20% yearly revenue loss * One-time financial cost > $1M * Uncorrectable errors in funding and personnel | * Yearly operational costs up 2-15% * 5-20% yearly revenue loss * One-time financial cost of $25K to $1M * Partially correctable errors in funding and personnel | * Increase of less than 2% in operating costs * <5% yearly revenue loss * One-time financial cost of <$25K * Inconvenient but correctable errors in funding and personnel |

### Scheduling Data Worksheet A7.3 Evaluate the Impacts of Threats to Critical Assets

**Human Actors Using Network Access After GAP Analysis**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Low |
|  |  |  |  |  |  | accidental |  | modification |  | Medium |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Low |
|  |  |  |  |  |  | deliberate |  | modification |  | Medium |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |
| Scheduling |  | network |  |  |  |  |  |  |  |  |
| Data |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Low |
|  |  |  |  |  |  | deliberate |  | modification |  | Medium |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  | Medium |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |
| Scheduling |  | physical |  |  |  |  |  |  |  |  |
| Data |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | Low |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | viruses |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
| Scheduling |  |  |  |  |  |  |
| Data |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  | Medium |
|  |  |  |  | interruption |  | Low |
| Scheduling |  |  |  |  |  |  |
| Data |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

## Research and Development Data

### Research and Development Data Worksheet A4.1 Critical Asset Information

|  |  |
| --- | --- |
| **Critical Asset Information** | |
| Asset | Research and Development Data |
| **Rationale for selection as a critical asset** | Swisher creates mostly custom products for clients, and therefore undergo heavy R&D to create those products. Most products require R&D. |
| **Brief description** | * Research and development data are stored within the lab system, which is isolated from the rest of the network. * Research and development data undergo simulations before being sent to the production system.   Research and development data are crucial to Swisher as almost all of their clients order custom built products. That means that Swisher needs to create and test new products in house before making them. The research and development lab allow for simulations of the data to determine whether it will pass as a successful product or not before handing the data to the production system to produce. |

### Research and Development Data Worksheet A4.2 Security Requirements Group Worksheet

| **Security Requirement Type** | **Priority** | **Specific Requirement** |
| --- | --- | --- |
| Confidentiality | X | Research and development data need to be kept confidential at all times.  Research and development data will be restricted on a “need to know” basis, and restricted to authorized personnel only. |
| Integrity |  | Research and development data must be kept accurate and unmodified.  Only authorized personnel should be allowed to modify the data. |
| Availability |  | Access to the research and development data should be available during business operation hours to authorized personnel only. |
| Other |  |  |

### Research and Development Data Worksheet W4.2 Security Requirements Group Worksheet

| Security Requirements Group | |
| --- | --- |
| Asset: Research and Development Data | |
| Security Requirements  (\* indicates most important) | Security Requirements  (\* indicates most important) |
| Senior Management | Operational Area Management |
| AVAILABILITY\*   * R&D data should be available 24/7 to authorized personnel.   CONFIDENTIALITY\*   * R&D data should be confidential at all times and only available to authorized personnel.   INTEGRITY   * R&D data may only be modified by authorized personnel. | AVAILABILITY   * R&D data should be available 24/7 to authorized personnel.   CONFIDENTIALITY\*   * R&D data should be confidential at all times and only available to authorized personnel.   INTEGRITY\*   * R&D data may only be modified by authorized personnel. |
| Staff | IT Staff |
| AVAILABILITY  CONFIDENTIALITY  INTEGRITY | AVAILABILITY   * R&D data should be available 24/7 to authorized personnel.   CONFIDENTIALITY\*   * R&D data should be confidential at all times and only available to authorized personnel.   INTEGRITY   * R&D data may only be modified by authorized personnel. |

### Research and Development Data Worksheet W4.3 Areas of Concern

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Research and Development Data** | |
| *Senior Management Area of Concern* | *Impact* |
| (1.1) Leaked research and development data. There are too many people who have access to the lab system. | This would be horrible as at Swisher’s, we typically build custom products for our clients. If competitors get a hold of what we are developing or our R&D data, they could attempt to replicate it and steal our clients.  Access – Physical  Actor – Inside  Motive – Accidental  Outcome – Disclosure |
| (1.2) Research and development expenditures exceeding projections. We always create a projection for our research and development and calculate the expenditures when discussing with a client. One concern is that the expenditures exceed what was discussed and we pay more out of pocket. | Additional costs at the expense of Swisher’s due to unexpected expenditures of R&D.  Access – N/A  Actor – Third-party problems or unavailability of their-party systems  Motive – N/A  Outcome – Loss, destruction; Interruption |
| (1.3) Storage location and back-up of R&D data. Not sure whether it is backed up or not, and where it would be located. If a catastrophic failure were to happen, it would be lost if there is no back-up. | Complete loss of R&D data would cripple Swisher as they would need to start from scratch to make a client’s product. This in turn would delay delivery and require additional expenses from Swisher.  Access – N/A  Actor – System crashes  Motive – N/A  Outcome – Loss, destruction |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Research and Development Data** | |
| *Operational Area Management Area of Concern* | *Impact* |
| (2.1) Someone stealing the research and development designs, as the data is usually out in plain sight such as on the computer screens or whiteboards in the lab. | Stolen design is usually with ill intent, and in this case, would most likely be by our competitors. They can use our designs to improve their own production and take away our clients.  Access – Physical  Actor – Inside; Outside  Motive – Deliberate  Outcome – Disclosure |
| (2.2) Someone coming into the lab and modifying the integrity of the data. There are too many unauthorized individuals that come into the lab. | Modification of R&D data would mean we need to start from scratch, which inevitably delays the production and delivery of the final product to our clients.  Access – Physical  Actor – Inside; Outside  Motive – Deliberate  Outcome – Modification |
| (2.3) Backup systems failing and not backing up critical research and development data. | If we lost our R&D data and did not have backups in place, then we would need to start from scratch. Delaying the production of the final product.  Access – N/A  Actor – Hardware defects  Motive – N/A  Outcome – Loss, destruction |
| (2.4) Not having the ability for backups to be done. Similar, but not failing backup systems, but rather inability to produce backups, as simulations tend to run throughout the week in the lab, so the IT staff can only do backups on Saturdays. | The inconsistent backups put the efforts of the recent R&D data at risk to any potential complications. This would mean R&D data would have to be created from scratch and delay production of the final product.  Access – N/A  Actor – Telecommunications problems or unavailability  Motive – N/A  Outcome – Loss, destruction; Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Research and Development Data** | |
| *Staff Area of Concern* | *Impact* |
| (3.1) The research and development data coming from the lab being inaccurate. This gets fed to the automated production process. | Having incorrect R&D data would cause the wrong product to be produced, delaying production of the product and destroying material.  Access – Network  Actor – Inside; Software defects  Motive – Accidental  Outcome – Loss, destruction; Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Research and Development Data** | |
| *IT Staff Area of Concern* | *Impact* |
| (4.1) Too many people have access to the lab system. The lab system contains the research and development data. | Loss of research and development data would mean we lose are competitive edge in our market.  Access – Physical  Actor – Inside  Motive – Accidental  Outcome – Disclosure |
| (4.2) Modified research and development data, also due to too many individuals in the lab system that do not need to be there. | Modified R&D data would need to be remade from scratch, delaying the production of the final products.  Access – Physical  Actor – Inside  Motive – Accidental  Outcome – Modification |

### Research and Development Data Worksheet A4.3 Threat Trees

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  | (3.1) |
|  |  |  |  |  |  |  |  | interruption |  | (3.1) |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
| R&D |  | network |  |  |  |  |  |  |  |  |
| Data |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

* (3.1) Concerned with improper R&D data being fed into the automated production system.
* The R&D data is inside the lab system which is completely isolated, so network access would be very difficult unless the individual was a staff member with access to the lab system.

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | (1.1), (4.1) |
|  |  |  |  |  |  | accidental |  | modification |  | (4.2) |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | (2.1) |
|  |  |  |  |  |  | deliberate |  | modification |  | (2.2) |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
| R&D |  | physical |  |  |  |  |  |  |  |  |
| Data |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | (2.1) |
|  |  |  |  |  |  | deliberate |  | modification |  | (2.2) |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  | (3.1) |
|  |  |  |  | interruption |  | (3.1) |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | viruses |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
| R&D |  |  |  |  |  |  |
| Data |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  | (1.3) |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  | (2.3) |
|  |  |  |  | interruption |  |  |

**Note**:

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  | (2.4) |
|  |  |  |  | interruption |  | (2.4) |
| R&D |  |  |  |  |  |  |
| Data |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  | (1.2) |
|  |  | third-party systems |  | interruption |  | (1.2) |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

**Note**:

* (1.2) Concerned with miscalculated expenditures, resulting in unexpected expenses.
* (2.4) Concerned with the inability to create backups of the R&D during specific windows of time.

### Research and Development Data Worksheet A5.1 Identify Key Classes of Components

|  |  |
| --- | --- |
| **Research and Development Data** | |
| **Class of Component** | **Rationale for Selection** |
| * Servers | R&D data is stored in the lab servers. |
| * Networking components | Routers and switches are required to grant internal and access. |
| * Security components | Encryption standards in place to ensure confidentiality and integrity of the data. |
| * Desktop workstations | Used to run simulations as well as create designs. |
| * Home computers |  |
| * Laptops |  |
| * Storage devices | Used to store R&D data. |
| * Wireless components |  |
| * Others (list)   3D printer | Used to print prototypes. |

### Research and Development Data Worksheet A5.2 Identify Infrastructure Components to Examine

| **Class of Component** | **Selected Component/ IP Addresses/Host Names** | **Rationale** | **Approach** |
| --- | --- | --- | --- |
| System of interest | Research and Development Lab System | The research and development data are what Swisher uses to develop custom products for their customers. | Performance of pass/fail audits on specific components related to Research and Development Data. |
| Systems/servers | Lab System Servers | Contain vital processes and instructions related to R&D data. | The IT Staff will test the confidentiality and integrity of the lab system servers.  1. Verify that all software and programs are up to date.  2. Verify the logs to ensure only authorized personnel have been on the server.  3. Verify that only authorized modifications to the server were made.  4. Verify that only necessary ports are open and vulnerable ones are closed.  5. Verify that there are physical barriers and a door that has a functioning locking mechanism with a pin pad in place.  6. Verify there is a backup schedule. |
| Networking components | Routers and Switches | Even though the Lab System is isolated, the machines inside need to communicate with each other and reach the Internet for resources. | The IT Staff will test whether the routers and switches are configured properly.  1. Verify that the routers are configured to use NAT.  2. Verify that all device connected to the routers and switches are registered.  3. Verify that router log is sent back to the syslog server.  4. Verify that the router has a unique username and password from the default.  5. Verify that all routers and switches are locked behind a physical barrier. |
| Security components | Encryption Methods | R&D data should be kept confidential, and an encryption method would be the best way to do that. | The IT Staff will test whether the R&D data is properly encrypted or not.  1. Verify that VeraCrypt is installed on the workstations that have R&D data on it.  2. Verify that all files with R&D data are encrypted with VeraCrypt.  3. Verify that authorized staff who use the lab workstations to modify inventory data are using VeraCrypt properly. |
| Desktop workstations | Lab Workstations | These workstations are required to perform research, design products, and run simulations. | The IT Staff will test lab workstations for possible vulnerabilities.  1. Verify that all staff are using a strong password by running Jack the Ripper on a VM for 24 hours.  2. Verify that there is no software installed on workstations that do not pertain to work.  3. Verify that there are screensavers in place when the workstation is left unattended for 3 minutes.  4. Verify that files with important data are encrypted using VeraCrypt.  5. Verify that workstations do not have keyloggers attached. |
| Home computers | N/A | N/A | N/A |
| Laptops | N/A | N/A | N/A |
| Storage devices | Network Attached Storage | This is not attached to the entire Swisher network, but the isolated network within the lab system so machines can communicate with each other. | The IT Staff will test the network attached storage for vulnerabilities and ensure that it is able to keep data confidential and available.  1. Verify that the NAS software is up to date.  2. Verify that the default administrator account is disabled.  3. Verify there is a firewall in place.  4. Verify that all NAS are locked behind a physical barrier.  5. Verify there is a backup schedule. |
| Wireless components | N/A | N/A | N/A |
| Others | 3D Printers | This is what Swisher uses to print prototypes. The calibrations and settings need to be correctly tuned to the specific task at hand. | The IT Staff will test to see if the 3D printers have any vulnerabilities.  1. Verify that the 3D printers are not connected to the Internet.  2. Verify that materials are able to withstand extrusion heat and will not cause a fire hazard. |

### Research and Development Data Worksheet A6.1 Review Technology Vulnerabilities and Summarize Results

| **Asset: Research and Development Data** | | | | |
| --- | --- | --- | --- | --- |
| **Class** | **Selected Component/ IP Address/Host Name** | **Results** | **Vulnerability Summary** | |
| Systems/  servers | Lab System Servers | 1. Pass  2. Pass  3. Fail  4. Pass  5. Pass  6. Pass | - medium | |
| Networking  component | Routers and Switches | 1. Pass  2. Pass  3. Fail  4. Fail  5. Pass | - low  - medium | |
| Security  component | Encryption Methods | 1. Pass  2. Pass  3. Pass | N/A | |
| Desktop  workstation | Lab Workstations | 1. Fail  2. Fail  3. Pass  4. Pass  5. Pass | - medium  - low | |
| Storage  devices | Network Attached Storage | 1. Pass  2. Fail  3. Pass  4. Fail  5. Pass | - medium  - low | |
| Others | 3D Printers | 1. Pass  2. Pass | N/A | |
| **Actions and Recommendations for Addressing Technology Vulnerabilities** | | | |
| **Company-wide Vulnerabilities** | | | |
| Routers and Switches – The devices that connect to the router and switches are not all registered. Unregistered devices may not belong to staff, which can pose serious risks as the individual is now within Swisher’s network. The other vulnerability is physical, in the fact that the routers and switches are not locked away in a physical container/barrier of sorts. Both of these vulnerabilities are of low severity and can be fixed at a later day. | | | |
| Firewalls – The firewalls are assigned to the production and inventory systems. The only vulnerability is of medium severity, and that is because the access control list is not up to date. This can allow unwanted data packets from entering the network and the systems. | | | |
| Network Attached Storage – NAS is used across the network, but the lab system that holds the R&D data have a separate one. There is one medium and two low severities. The medium is the NAS software is not up to date. Update contain various security patches that keep the NAS device from known vulnerabilities. The two lows are that there is no firewall in place, and there is no physical barrier protecting the NAS. Firewalls help protect the data on the NAS device by filtering traffic in and out. No physical barriers could mean someone could gain access to the NAS device rather easily. | | | |

|  |
| --- |
| **Actions and Recommendations for Addressing Technology Vulnerabilities** |
| **Research and Development Data** |
| Lab System Servers – The lab system servers have one medium severity issue. The medium severity issue is that non-authorized modifications were made on the server. Non-authorized modifications can lead to an integrity and availability issue. |
| Lab Workstations – The lab workstations have one medium and one low severity issue. The medium severity issue that the staff is using weak passwords. Weak passwords are easy to compromise, and thus a password policy should be created. The low severity issue pertains with unnecessary software on the workstation. This software could possibly have malicious content on them. It is best to not download anything that doesn’t pertain to work on workstations at Swisher. |

### Research and Development Data Worksheet A7.1 Identify the Impact of Threats to Critical Assets

| **Research and Development Data** | | | |
| --- | --- | --- | --- |
| **Impacts to the Organization** | | | |
| **Outcome** | **Consider** | **Impact Descriptions** | **Values** |
| **Disclosure** | * How could the organization’s reputation be affected if this asset were disclosed? * How could customer confidence be affected if this asset were disclosed? * How could the health of customers be affected if this asset were disclosed? * How could employee productivity be affected if this asset were disclosed? * How would other users of this asset be affected if this asset were disclosed? * What fines, legal penalties, or lawsuits could be imposed as a result of disclosure of this asset? * How could the organization be affected financially if this asset were disclosed? * What other impacts could occur if this asset were disclosed? For example: * ethical considerations * other legal/financial impacts | * If scheduling data were to be disclosed, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect their information that may be in the company. Additionally, other businesses that may have gotten a hold of Swisher’s R&D could become more competitive from the information stolen. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the research and development data were disclosed because it means that Swisher does not have the means to protect their information assets. * Disclosure of the research and development data has no ill effect on customer’s health. * Disclosure of the research and development data may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the research and development data more secure. * Users of the research and development data would not be affected as disclosure means that the information was leaked/taken. It does not change the integrity of the research and development data. * Disclosure of the research and development data would mean possible disclosure of customer information related to the product Swisher is commissioned to develop. This would be a breach in consumer data privacy laws such as the GDPR for European customers and the US Privacy Act of 1974 for US customers. * Disclosure of the research and development data would mean losing the competitive edge Swisher has in the market due to their custom products. This could result in a loss of customers attracted to competitors. * All considerations to disclosure of impacts have been made in relation to Swisher’s research and development data. |  |
| **Modification** | * How could the organization’s reputation be affected if this asset were modified? * How could customer confidence be affected if this asset were modified? * How could the health of customers be affected if this asset were modified? * How could employee productivity be affected if this asset were modified? * How would other users of this asset be affected if this asset were modified? * What fines, legal penalties, or lawsuits could be imposed as a result of modification of this asset? * How could the organization be affected financially if this asset were modified? * What other impacts could occur if this asset were modified? For example: * ethical considerations * other legal/financial impacts | * If research and development data were to be modified, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect the integrity of their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the research and development data were disclosed because it means that Swisher does not have the means to protect their information assets. * Modification of the research and development data may impact customers and their clients if the R&D were to have their design modified. Sickness, injury, or death are possibilities of an inappropriately designed product. * Disclosure of the research and development data may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the research and development data more secure. * There are no other users of the research and development data other than the staff at Swisher. * Modification of the research and development data would mean possible modification of customer information related to the product Swisher is commissioned to develop. This would be a breach in consumer data privacy laws such as the GDPR for European customers and the US Privacy Act of 1974 for US customers. * Modification of the research and development data would mean losing the competitive edge Swisher has in the market due to their custom products. This could result in a loss of customers attracted to competitors. * All considerations to modification of impacts have been made in relation to Swisher’s research and development data. |  |
| **Destruction/Loss** | * How could the organization’s reputation be affected if this asset were destroyed, lost, or unavailable? * How could customer confidence be affected if this asset were destroyed, lost, or unavailable? * How could the health of customers be affected if this asset were destroyed, lost, or unavailable? * How could employee productivity be affected if this asset were destroyed, lost, or unavailable? * How would other users of this asset be affected if this asset were destroyed, lost, or unavailable? * What fines, legal penalties, or lawsuits could be imposed as a result of destruction/loss of this asset? * How could the organization be affected financially if this asset were destroyed, lost, or unavailable? * What other impacts could occur if this asset were destroyed, lost, or unavailable? For example: * ethical considerations * other legal/financial impacts | * If scheduling data were to be destroyed/lost, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the research and development data were destroyed/lost because it means that Swisher does not have the means to protect their information assets. * Destruction/loss of the research and development data has no ill effect on customer’s health. * Destruction/loss of the research and development data may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the research and development data more secure. * There are no other users of the research and development data other than the staff at Swisher. * Destruction/loss of the research and development data at Swisher’s does not breach any laws or regulations and not subject to legal penalties. * Destruction/loss of the research and development data would mean losing the competitive edge Swisher has in the market due to their production processes. This could result in a loss of customers attracted to competitors. * All considerations to destruction/loss of impacts have been made in relation to Swisher’s research and development data. |  |
| **Interruption** | * How could the organization’s reputation be affected if access to this asset were unavailable? * How could customer confidence be affected if access to this asset were unavailable? * How could the health of customers be affected if access to this asset were unavailable? * How could employee productivity be affected if access to this asset were unavailable? * How would other users of this asset be affected if access to this asset were unavailable? * What fines, legal penalties, or lawsuits could be imposed as a result of unavailability of this asset? * How could the organization be affected financially if access to this asset were unavailable? * What other impacts could occur if access to this asset were unavailable? For example: * ethical considerations * other legal/financial impacts | * If research and development data were to be unavailable, clients may view Swisher’s cyber security to be deficient, and may not be able to protect their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the research and development data were unavailable because it means that Swisher does not have the means to protect their information assets. * Unavailability of the research and development data has no ill effect on customer’s health. * Unavailability of the research and development data may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the research and development data more secure. * There are no other users of the research and development data other than the staff at Swisher. * Unavailability of the research and development data at Swisher’s does not breach any laws or regulations and not subject to legal penalties. * Unavailability of the research and development data would mean losing the competitive edge Swisher has in the market due to their production processes. This could result in a loss of customers attracted to competitors. * All considerations to unavailability of impacts have been made in relation to Swisher’s research and development data. |  |

### Research and Development Data Worksheet A7.2 Create Risk Evaluation Criteria

| Research and Development Data Evaluation Criteria | | | |
| --- | --- | --- | --- |
| **Impact Area** | **High** | **Medium** | **Low** |
| Reputation/ Customer Confidence | * Reputation irrevocably destroyed or damaged * More than 30% drop in customers due to loss of confidence | * Reputation damaged; some effort and expense required to recover * 10 to 30% drop in customers due to loss of confidence * Customer goes to competitor | * Reputation minimally affected; little or no effort or expense required to recover * Less than 10% drop in customers due to loss of confidence |
| Life/ Health of Customers | * Loss of customer life * Permanent impairment of one or more significant aspects of customer’s health (e.g., loss of use of one or more limbs, blindness, brain damage) * Safety violated | * Customer life threatened but recoverable with additional treatment * Temporary or recoverable impairment of customer’s health (e.g., recovering use of limbs through physical therapy) * Safety affected | * No loss or significant threat to customer life * Minimal, immediately treatable degradation in customer heath with recovery within four days * Safety questioned |
| Productivity | * Staff unable to perform critical job aspects for three or more days * 40% or more increase in work hours required of at least 10% of general staff for > three days * Irrecoverable loss of server data | * Staff work increased by 10-40% for one day * Increases in general staff work of 10-40% for one day * Inefficient continuity of availability; delays while recovering misplaced information | * Staff inconvenienced for less than a day but no measurable increase in work effort occurs * General staff inconvenienced for less than a day but no measurable increase in work effort occurs |
| Fines/ Legal Penalties | * Fines of greater than $100,000 levied * One or more non-frivolous lawsuits of more than $3,000,000 filed by customers * Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices | * Fines of $10,000 to $100,000 levied * One or more non-frivolous lawsuits between $250,000 and $3,000,000 filed by customers * Government or other investigative organization requests information or records (low-profile) | * No fine or a fine of less than $10,000 levied * Lawsuit of less than $250,000 or frivolous lawsuit (95% sure it can be defeated) filed by customer * No queries from government or other investigative organizations |
| Finances | * Yearly operational costs up 15% * 20% yearly revenue loss * One-time financial cost > $1M * Uncorrectable errors in funding and personnel | * Yearly operational costs up 2-15% * 5-20% yearly revenue loss * One-time financial cost of $25K to $1M * Partially correctable errors in funding and personnel | * Increase of less than 2% in operating costs * <5% yearly revenue loss * One-time financial cost of <$25K * Inconvenient but correctable errors in funding and personnel |

### Research and Development Data Worksheet A7.3 Evaluate the Impacts of Threats to Critical Assets

**Human Actors Using Network Access After GAP Analysis**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | High |
|  |  |  |  |  |  | accidental |  | modification |  | High |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | High |
|  |  |  |  |  |  | deliberate |  | modification |  | High |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |
| R&D |  | network |  |  |  |  |  |  |  |  |
| Data |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | High |
|  |  |  |  |  |  | deliberate |  | modification |  | High |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | High |
|  |  |  |  |  |  | accidental |  | modification |  | High |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | High |
|  |  |  |  |  |  | deliberate |  | modification |  | High |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
| R&D |  | physical |  |  |  |  |  |  |  |  |
| Data |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | High |
|  |  |  |  |  |  | deliberate |  | modification |  | High |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  | interruption |  | Low |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | viruses |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
| R&D |  |  |  |  |  |  |
| Data |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  | interruption |  |  |

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  | Medium |
|  |  |  |  | interruption |  | Low |
| R&D |  |  |  |  |  |  |
| Data |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  | Medium |
|  |  | third-party systems |  | interruption |  | Low |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

## Inventory System

### Inventory System Worksheet A4.1 Critical Asset Information

|  |  |
| --- | --- |
| **Critical Asset Information** | |
| Asset | Inventory System |
| **Rationale for selection as a critical asset** | The inventory system is responsible for having the right materials ready for production. Swisher’s makes custom products for clients, and that requires the proper materials to build. Without the correct material, it puts stress on production machines and creates a suboptimal product. |
| **Brief description** | * Contains all information on materials to be used. * Inventory system is responsible for ordering the correct materials for upcoming and current products. * Inventory data exists in both the production and administrative systems.   Swisher’s inventory system comprises of the inventory data. It works in conjunction with the scheduling system to get orders in. Inventory data accounts for material that is used for current and upcoming products. It directly ties with the accounting system as it affects the billing cycle depending on what materials have been ordered. |

### Inventory System Worksheet A4.2 Security Requirements Group Worksheet

| **Security Requirement Type** | **Priority** | **Specific Requirement** |
| --- | --- | --- |
| Confidentiality |  | The inventory system needs to be kept confidential at all times.  The inventory system will be restricted on a “need to know” basis, and restricted to authorized personnel only. |
| Integrity | X | The inventory system must be kept accurate and unmodified.  Only authorized personnel should be allowed to modify the data on the inventory system. |
| Availability |  | Access to the inventory system should available 24/7 to authorized personnel only. |
| Other |  |  |

### Inventory System Worksheet W4.2 Security Requirements Group Worksheet

| Security Requirements Group | |
| --- | --- |
| Asset: Inventory System | |
| Security Requirements  (\* indicates most important) | Security Requirements  (\* indicates most important) |
| Senior Management | Operational Area Management |
| AVAILABILITY   * The inventory system should be available 24/7 to authorized personnel.   CONFIDENTIALITY   * The inventory system should be confidential at all times and only available to authorized personnel.   INTEGRITY\*   * The inventory system may only be modified by authorized personnel. | AVAILABILITY\*   * The inventory system should be available 24/7 to authorized personnel.   CONFIDENTIALITY   * The inventory system should be confidential at all times and only available to authorized personnel.   INTEGRITY\*   * The inventory system may only be modified by authorized personnel. |
| Staff | IT Staff |
| AVAILABILITY   * The inventory system should be available 24/7 to authorized personnel.   CONFIDENTIALITY\*   * The inventory system should be confidential at all times and only available to authorized personnel.   INTEGRITY\*   * The inventory system may only be modified by authorized personnel. | AVAILABILITY  CONFIDENTIALITY  INTEGRITY |

### Inventory System Worksheet W4.3 Areas of Concern

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Inventory System** | |
| *Senior Management Area of Concern* | *Impact* |
| (1.1) Running out of specific materials due to a complication in the inventory system. | This would create a delay in the delivery date of the final product to our client. Potentially losing us a client.  Access – N/A  Actor – Software defects  Motive – N/A  Outcome – Interruption |
| (1.2) Use of other materials in place of unavailable materials for a product. | Using different materials will take it away from what it actually needed for. The final product may be inferior and not meet the client’s satisfactions, thus, potentially losing them as a client.  Access – Physical  Actor – Inside  Motive – Deliberate  Outcome – Modification; Loss, destruction; Interruption |
| (1.3) Damaged machines due to use of other materials for building a product. | Certain materials may be harder than others, and when used as a substitute, they can damage the machines. If machines are damaged too much, they need to be repaired or replaced. Costing us time and money.  Access – N/A  Actor – Hardware defects  Motive – N/A  Outcome – Loss, destruction; Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Inventory System** | |
| *Operational Area Management Area of Concern* | *Impact* |
| (2.1) Failure of clerks moving products in and out of inventory and forgetting to complete the receipt. Affecting billing because accounting is not made aware of the product movement. | Clients don’t get billed until products go into inventory and then shipped. If the billing cycle is over, then it overlaps into next month’s bill. We do not get paid until later then.  Access – Physical  Actor – Inside  Motive – Accidental  Outcome – Interruption |
| (2.2) Delays in the inventory ordering system. Ordering products and materials from vendors and the order doesn’t get processed quickly, it delays our payment to the vendors. | Delayed payment usually incurs late fees that we have to pay. Which are more expenses for us.  Access – Network  Actor – Inside; Third-party problems or unavailability of third-party systems  Motive – Accidental  Outcome – Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Inventory System** | |
| *Staff Area of Concern* | *Impact* |
| (3.1) Errors in inventory data which affects accounting, due to the nature of purchasing materials and billing for products. | Would cost Swisher late fees as well as not being able to provide clients with information on the progress of the product.  Access – N/A  Actor – Software defects  Motive – N/A  Outcome – Interruption |
| (3.2) Lack of availability of the inventory system, as it tells us what is being used and what is available, material-wise. | Won’t be able to produce products without information from the inventory system.  Access – N/A  Actor – Telecommunications problems or unavailability  Motive – N/A  Outcome – Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: Inventory System** | |
| *IT Staff Area of Concern* | *Impact* |
| N/A | N/A |

### Inventory System Worksheet A4.3 Threat Trees

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  | (2.2) |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
| Inventory |  | network |  |  |  |  |  |  |  |  |
| System |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  | (2.1) |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  | (1.2) |
|  |  |  |  |  |  |  |  | loss, destruction |  | (1.2) |
|  |  |  |  |  |  |  |  | interruption |  | (1.2) |
| Inventory |  | physical |  |  |  |  |  |  |  |  |
| System |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | (1.1), (3.1) |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | viruses |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
| Inventory |  |  |  |  |  |  |
| System |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  | (1.3) |
|  |  |  |  | interruption |  | (1.3) |

**Note**:

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | (3.2) |
| Inventory |  |  |  |  |  |  |
| System |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  | (2.2) |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

**Note**:

### Inventory System Worksheet A5.1 Identify Key Classes of Components

|  |  |
| --- | --- |
| **Inventory System** | |
| **Class of Component** | **Rationale for Selection** |
| * Servers | Inventory data is stored in the inventory servers. |
| * Networking components | Routers and switches are required to grant internal and access. |
| * Security components | Firewalls in place at routers that connect to the Internet. |
| * Desktop workstations | Used to place and update orders. |
| * Home computers |  |
| * Laptops |  |
| * Storage devices | Used to store inventory data. |
| * Wireless components |  |
| * Others (list)   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

### Inventory System Worksheet A5.2 Identify Infrastructure Components to Examine

| **Class of Component** | **Selected Component/ IP Addresses/Host Names** | **Rationale** | **Approach** |
| --- | --- | --- | --- |
| System of interest | Inventory System | The inventory system contains data on materials ordered, in storage, and products to be shipped. | Performance of pass/fail audits on specific components related to the Inventory System. |
| Systems/servers | Inventory System Servers | Contain vital processes and instructions related to the inventory system. | The IT Staff will test the confidentiality and integrity of the inventory system servers.  1. Verify that all software and programs are up to date.  2. Verify the logs to ensure only authorized personnel have been on the server.  3. Verify that only authorized modifications to the server were made.  4. Verify that only necessary ports are open and vulnerable ones are closed.  5. Verify that there are physical barriers and a door that has a functioning locking mechanism with a pin pad in place.  6. Verify there is a backup schedule. |
| Networking components | Routers and Switches | These devices act as the connection points where data must travel through | The IT Staff will test whether the routers and switches are configured properly.  1. Verify that the routers are configured to use NAT.  2. Verify that all device connected to the routers and switches are registered.  3. Verify that router log is sent back to the syslog server.  4. Verify that the router has a unique username and password from the default.  5. Verify that all routers and switches are locked behind a physical barrier. |
| Security components | Firewalls | Used to filter incoming and outgoing traffic from the systems to the Internet. | The IT Staff will test that the firewall is properly configured.  1. Verify that the access control list is up to date.  2. Verify that the firewall is sending logs to the syslog server.  3. Verify that the firewall has a unique username and password from the default. |
| Desktop workstations | Inventory Workstations | Used to place and update orders. | The IT Staff will test inventory workstations for possible vulnerabilities.  1. Verify that all staff are using a strong password by running Jack the Ripper on a VM for 24 hours.  2. Verify that there is no software installed on workstations that do not pertain to work.  3. Verify that there are screensavers in place when the workstation is left unattended for 3 minutes.  4. Verify that files with important data are encrypted using VeraCrypt.  5. Verify that workstations do not have keyloggers attached. |
| Home computers | N/A | N/A | N/A |
| Laptops | N/A | N/A | N/A |
| Storage devices | Network Attached Storage | Used to store inventory data such as materials in stock, pending orders, customer and vendor contacts. | The IT Staff will test the network attached storage for vulnerabilities and ensure that it is able to keep data confidential and available.  1. Verify that the NAS software is up to date.  2. Verify that the default administrator account is disabled.  3. Verify there is a firewall in place.  4. Verify that all NAS are locked behind a physical barrier.  5. Verify there is a backup schedule. |
| Wireless components | N/A | N/A | N/A |
| Others | N/A | N/A | N/A |

### Inventory System Worksheet A6.1 Review Technology Vulnerabilities and Summarize Results

| **Asset: Inventory System** | | | |
| --- | --- | --- | --- |
| **Class** | **Selected Component/ IP Address/Host Name** | **Results** | **Vulnerability Summary** |
| Systems/  servers | Inventory System Servers | 1. Fail  2. Fail  3. Fail  4. Pass  5. Pass  6. Fail | - medium  - high  - medium  - low |
| Networking  component | Routers and Switches | 1. Pass  2. Fail  3. Pass  4. Pass  5. Fail | - low  - low |
| Security  component | Firewalls | 1. Fail  2. Pass  3. Pass | - medium |
| Desktop  workstations | Inventory Workstations | 1. Pass  2. Pass  3. Fail  4. Pass  5. Pass | - low |
| Storage  devices | Network Attached Storage | 1. Fail  2. Pass  3. Fail  4. Fail  5. Pass | - medium  - low  - low |

|  |
| --- |
| **Actions and Recommendations for Addressing Technology Vulnerabilities** |
| **Company-wide Vulnerabilities** |
| Routers and Switches – The devices that connect to the router and switches are not all registered. Unregistered devices may not belong to staff, which can pose serious risks as the individual is now within Swisher’s network. The other vulnerability is physical, in the fact that the routers and switches are not locked away in a physical container/barrier of sorts. Both of these vulnerabilities are of low severity and can be fixed at a later day. |
| Firewalls – The firewalls are assigned to the production and inventory systems. The only vulnerability is of medium severity, and that is because the access control list is not up to date. This can allow unwanted data packets from entering the network and the systems. |
| Network Attached Storage – NAS is used across the network, but the lab system that holds the R&D data have a separate one. There is one medium and two low severities. The medium is the NAS software is not up to date. Update contain various security patches that keep the NAS device from known vulnerabilities. The two lows are that there is no firewall in place, and there is no physical barrier protecting the NAS. Firewalls help protect the data on the NAS device by filtering traffic in and out. No physical barriers could mean someone could gain access to the NAS device rather easily. |

|  |
| --- |
| **Actions and Recommendations for Addressing Technology Vulnerabilities** |
| **Inventory System** |
| Inventory System Servers – The inventory system servers have one high, two medium, and one low severity issues. The high severity issue is that there are unauthorized personnel on the server, which could lead to many issues such as confidentiality of data, integrity of data, as well as availability of the server. The two medium severity issues are that the software on the server is not update and non-authorized modifications were made on the server. The latest software updates usually contain security patches to protect against known vulnerabilities in the software. Non-authorized modifications can lead to an integrity and availability issue. The low severity issue is that there are no backups scheduled for the server. Though preferable, the lack of a backup is not an immediate threat to Swisher. A backup is recommended, however, as system crashes or incidents where data is lost may occur. |
| Inventory Workstations – The inventory workstations have one low severity issue. The low severity issue is that the staff do not have screensavers that meet a 3-minute requirement. Screensavers help protect the information on a workstation if one forgets to lock their screen, otherwise, others can use the workstation in its current session. |

### Inventory System Worksheet A7.1 Identify the Impact of Threats to Critical Assets

| **Inventory System** | | | |
| --- | --- | --- | --- |
| **Impacts to the Organization** | | | |
| **Outcome** | **Consider** | **Impact Descriptions** | **Values** |
| **Disclosure** | * How could the organization’s reputation be affected if this asset were disclosed? * How could customer confidence be affected if this asset were disclosed? * How could the health of customers be affected if this asset were disclosed? * How could employee productivity be affected if this asset were disclosed? * How would other users of this asset be affected if this asset were disclosed? * What fines, legal penalties, or lawsuits could be imposed as a result of disclosure of this asset? * How could the organization be affected financially if this asset were disclosed? * What other impacts could occur if this asset were disclosed? For example: * ethical considerations * other legal/financial impacts | * If the inventory system were to be disclosed, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the inventory system were disclosed because it means that Swisher does not have the means to protect their information assets. * Disclosure of the inventory system has no ill effect on customer’s health. * Disclosure of the inventory system may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the inventory system more secure. * Users of the inventory system would not be affected as disclosure means that the information was leaked/taken. It does not change the integrity of the inventory system. * Disclosure of the inventory system would mean possible disclosure of customer and vendor information. This would be a breach in consumer data privacy laws such as the GDPR for European customers and the US Privacy Act of 1974 for US customers. * Disclosure of the inventory system has little financial affect for Swisher. * All considerations to disclosure of impacts have been made in relation to Swisher’s inventory system. |  |
| **Modification** | * How could the organization’s reputation be affected if this asset were modified? * How could customer confidence be affected if this asset were modified? * How could the health of customers be affected if this asset were modified? * How could employee productivity be affected if this asset were modified? * How would other users of this asset be affected if this asset were modified? * What fines, legal penalties, or lawsuits could be imposed as a result of modification of this asset? * How could the organization be affected financially if this asset were modified? * What other impacts could occur if this asset were modified? For example: * ethical considerations * other legal/financial impacts | * If the inventory system were to be modified, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect the integrity of their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the inventory system were disclosed because it means that Swisher does not have the means to protect their information assets. * Modification of the inventory system may impact customers and their clients if the inventory data were to have their materials modified. Sickness, injury, or death are possibilities of the use of inappropriate materials for the product design. * Disclosure of the inventory system may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the inventory system more secure. * There are no other users of the inventory system other than the staff at Swisher. * Modification of the inventory system would mean possible modification of customer and vendor information. This would be a breach in consumer data privacy laws such as the GDPR for European customers and the US Privacy Act of 1974 for US customers. * Modification of the inventory system may impact Swisher’s financials if additional materials are ordered. * All considerations to modification of impacts have been made in relation to Swisher’s inventory system. |  |
| **Destruction/Loss** | * How could the organization’s reputation be affected if this asset were destroyed, lost, or unavailable? * How could customer confidence be affected if this asset were destroyed, lost, or unavailable? * How could the health of customers be affected if this asset were destroyed, lost, or unavailable? * How could employee productivity be affected if this asset were destroyed, lost, or unavailable? * How would other users of this asset be affected if this asset were destroyed, lost, or unavailable? * What fines, legal penalties, or lawsuits could be imposed as a result of destruction/loss of this asset? * How could the organization be affected financially if this asset were destroyed, lost, or unavailable? * What other impacts could occur if this asset were destroyed, lost, or unavailable? For example: * ethical considerations * other legal/financial impacts | * If the inventory system were to be destroyed/lost, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the inventory system were destroyed/lost because it means that Swisher does not have the means to protect their information assets. * Destruction/loss of the inventory system has no ill effect on customer’s health. * Destruction/loss of the inventory system may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the inventory system more secure. * There are no other users of the inventory system other than the staff at Swisher. * Destruction/loss of the inventory system at Swisher’s does not breach any laws or regulations and not subject to legal penalties. * Destruction/loss of the inventory system would mean losing the competitive edge Swisher has in the market due to their production processes. This could result in a loss of customers attracted to competitors. * All considerations to destruction/loss of impacts have been made in relation to Swisher’s inventory system. |  |
| **Interruption** | * How could the organization’s reputation be affected if access to this asset were unavailable? * How could customer confidence be affected if access to this asset were unavailable? * How could the health of customers be affected if access to this asset were unavailable? * How could employee productivity be affected if access to this asset were unavailable? * How would other users of this asset be affected if access to this asset were unavailable? * What fines, legal penalties, or lawsuits could be imposed as a result of unavailability of this asset? * How could the organization be affected financially if access to this asset were unavailable? * What other impacts could occur if access to this asset were unavailable? For example: * ethical considerations * other legal/financial impacts | * If inventory system were to be unavailable, clients as well as vendors may view Swisher’s cyber security to be deficient, and may not be able to protect their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the inventory system were unavailable because it means that Swisher does not have the means to protect their information assets. * Unavailability of the inventory system has no ill effect on customer’s health. * Unavailability of the inventory system may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the inventory system more secure. * There are no other users of the inventory system other than the staff at Swisher. * Unavailability of the inventory system at Swisher’s does not breach any laws or regulations and not subject to legal penalties. * Unavailability of the inventory system would mean losing the competitive edge Swisher has in the market due to their production processes. This could result in a loss of customers attracted to competitors. * All considerations to unavailability of impacts have been made in relation to Swisher’s inventory system. |  |

### Inventory System Worksheet A7.2 Create Risk Evaluation Criteria

| Inventory System Evaluation Criteria | | | |
| --- | --- | --- | --- |
| **Impact Area** | **High** | **Medium** | **Low** |
| Reputation/ Customer Confidence | * Reputation irrevocably destroyed or damaged * More than 30% drop in customers due to loss of confidence | * Reputation damaged; some effort and expense required to recover * 10 to 30% drop in customers due to loss of confidence * Customer goes to competitor | * Reputation minimally affected; little or no effort or expense required to recover * Less than 10% drop in customers due to loss of confidence |
| Life/ Health of Customers | * Loss of customer life * Permanent impairment of one or more significant aspects of customer’s health (e.g., loss of use of one or more limbs, blindness, brain damage) * Safety violated | * Customer life threatened but recoverable with additional treatment * Temporary or recoverable impairment of customer’s health (e.g., recovering use of limbs through physical therapy) * Safety affected | * No loss or significant threat to customer life * Minimal, immediately treatable degradation in customer heath with recovery within four days * Safety questioned |
| Productivity | * Staff unable to perform critical job aspects for three or more days * 40% or more increase in work hours required of at least 10% of general staff for > three days * Irrecoverable loss of server data | * Staff work increased by 10-40% for one day * Increases in general staff work of 10-40% for one day * Inefficient continuity of availability; delays while recovering misplaced information | * Staff inconvenienced for less than a day but no measurable increase in work effort occurs * General staff inconvenienced for less than a day but no measurable increase in work effort occurs |
| Fines/ Legal Penalties | * Fines of greater than $100,000 levied * One or more non-frivolous lawsuits of more than $3,000,000 filed by customers * Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices | * Fines of $10,000 to $100,000 levied * One or more non-frivolous lawsuits between $250,000 and $3,000,000 filed by customers * Government or other investigative organization requests information or records (low-profile) | * No fine or a fine of less than $10,000 levied * Lawsuit of less than $250,000 or frivolous lawsuit (95% sure it can be defeated) filed by customer * No queries from government or other investigative organizations |
| Finances | * Yearly operational costs up 15% * 20% yearly revenue loss * One-time financial cost > $1M * Uncorrectable errors in funding and personnel | * Yearly operational costs up 2-15% * 5-20% yearly revenue loss * One-time financial cost of $25K to $1M * Partially correctable errors in funding and personnel | * Increase of less than 2% in operating costs * <5% yearly revenue loss * One-time financial cost of <$25K * Inconvenient but correctable errors in funding and personnel |

### Inventory System Worksheet A7.3 Evaluate the Impacts of Threats to Critical Assets

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Low |
|  |  |  |  |  |  | accidental |  | modification |  | High |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Low |
|  |  |  |  |  |  | deliberate |  | modification |  | High |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |
| Inventory |  | network |  |  |  |  |  |  |  |  |
| System |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Low |
|  |  |  |  |  |  | deliberate |  | modification |  | High |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  | Low |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  | High |
|  |  |  |  |  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  |  |  |  |  | interruption |  | Low |
| Inventory |  | physical |  |  |  |  |  |  |  |  |
| System |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | Low |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | viruses |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
| Inventory |  |  |  |  |  |  |
| System |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  | Medium |
|  |  |  |  | interruption |  | Low |

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | Low |
| Inventory |  |  |  |  |  |  |
| System |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  | Low |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  |  |

## IT Staff

### IT Staff Worksheet A4.1 Critical Asset Information

|  |  |
| --- | --- |
| **Critical Asset Information** | |
| Asset | IT Staff |
| **Rationale for selection as a critical asset** | Swisher has gone years hiring a third-party tech support team for their systems, who did not have their best interest. The new IT administrator has gotten the entire system including networks to function properly. |
| **Brief description** | * Only one IT staff and that is the IT administrator. * Performs all IT related duties that Swisher requires.   The IT administrator was hired five years ago and has been an integral part of Swisher being able to perform as well as it has. Before, Swisher hired third party IT service which did not have Swisher’s best interest. Many jobs were done inappropriately as well as others being overlooked. The IT administrator has done a lot to the overall network and systems. |

### IT Staff Worksheet A4.2 Security Requirements Group Worksheet

| **Security Requirement Type** | **Priority** | **Specific Requirement** |
| --- | --- | --- |
| Confidentiality |  | The IT staff member will keep maintain confidentiality of the data on the network and systems such as intellectual property, R&D data, client data, etc.  The IT staff will be restricted on a need to know basis. |
| Integrity |  | The IT staff member will not modify any data on the network and systems unless given authorization. |
| Availability | X | The IT staff member should be available during their scheduled work hours. |
| Other |  |  |

### IT Staff Worksheet W4.2 Security Requirements Group Worksheet

| Security Requirements Group | |
| --- | --- |
| Asset: IT Staff | |
| Security Requirements  (\* indicates most important) | Security Requirements  (\* indicates most important) |
| Senior Management | Operational Area Management |
| AVAILABILITY\*   * Should be available during scheduled work hours.   CONFIDENTIALITY   * Maintain confidentiality of Swisher’s information assets.   INTEGRITY   * Modify only Swisher’s information assets on when authorized to do so. | AVAILABILITY\*   * Should be available during scheduled work hours.   CONFIDENTIALITY   * Maintain confidentiality of Swisher’s information assets.   INTEGRITY   * Modify only Swisher’s information assets on when authorized to do so. |
| Staff | IT Staff |
| AVAILABILITY\*   * Should be available during scheduled work hours.   CONFIDENTIALITY   * Maintain confidentiality of Swisher’s information assets.   INTEGRITY   * Modify only Swisher’s information assets on when authorized to do so. | AVAILABILITY  CONFIDENTIALITY  INTEGRITY |

### IT Staff Worksheet W4.3 Areas of Concern

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: IT Staff** | |
| *Senior Management Area of Concern* | *Impact* |
| (1.1) IT staff consists of one member and she does all IT related work. Afraid that she may leave because she is overworked. | Without a full-time IT staff member, the networks and systems would go back to their original state. We could lose a lot of clients just due to a lack of productivity because the system isn’t functioning well.  Access – Physical  Actor – Inside  Motive – Deliberate  Outcome – Interruption |
| (1.2) Not enough IT staff to cover second and third shifts. Current IT staff is pretty good answering on-call requests for second shift. | If a system or technical error was to occur during times that we do not have an IT staff to fix the issue, then we lost that entire shift or more of productivity.  Access – N/A  Actor – System crashes  Motive – N/A  Outcome – Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: IT Staff** | |
| *Operational Area Management Area of Concern* | *Impact* |
| (2.1) IT staff consists of one member and she does all IT related work. Afraid that she may leave because she is overworked. | If our only IT staff member leaves, then nobody is around to fix the production systems or do backups. This will revert us back to where we were without her, and we would lose so much productivity, which means less revenue for Swisher.  Access – Physical  Actor – Inside  Motive – Deliberate  Outcome – Interruption |
| (2.2) Failing to protect the IoT cameras and monitoring systems well enough. They are on a separate network, but it was hacked once before. | Hacked monitoring systems will allow the hacker to take confidential information or the layout of the building. They could also deny us access to the system and if an incident were to occur without our knowledge because we can’t see, then we could be in for a lawsuit if it is involving injury of a person who came on to Swisher’s property.  Access – Network  Actor – Outside; Physical configuration or arrangement of buildings, offices, or equipment  Motive – Deliberate  Outcome – Disclosure; Interruption |
| (2.3) Failure to backup research and development designs due to the stringent times of our simulations. | The inconsistent backups put the efforts of the recent R&D data at risk to any potential complications. This would mean R&D data would have to be created from scratch and delay production of the final product.  Access – N/A  Actor – Telecommunications problems or unavailability  Motive – N/A  Outcome – Interruption |
| (2.4) Failure to secure and backup human resources data. | All HR documents are confidential and should not be leaked, as it is a breach in privacy laws.  Access – Network  Actor – Inside  Motive – Accidental  Outcome – Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: IT Staff** | |
| *Staff Area of Concern* | *Impact* |
| (3.1) Only one IT staff and no one to give her support. If she ever gets sick, we will not have anyone in to take over her duties. | No one to manage the systems, causing a potential lack of productivity.  Access – Physical  Actor – Inside  Motive – Deliberate  Outcome – Interruption |
| (3.2) Taking away the production staff’s ability to view the status of the production process. | May delay the response to begin the next stages of the automated processes if the production staff does not know when the production process ends.  Access – Network; Physical  Actor – Inside  Motive – Deliberate  Outcome – Interruption |

|  |  |
| --- | --- |
| Areas of Concern Group | |
| **Asset: IT Staff** | |
| *IT Staff Area of Concern* | *Impact* |
| (4.1) If I ever get sick or injured, there is no one here to keep things operating as it should. | Lack of proper operations of systems would reduce productivity of Swisher’s.  Access – N/A  Actor – System crashes  Motive – N/A  Outcome – Interruption |
| (4.2) Lack of a contingency plan in the case of a disaster. No one has the skills or are trained to for a disaster. | Would completely take Swisher out of business if a large-scale disaster were to happen.  Access – N/A  Actor – Natural disasters  Motive – N/A  Outcome – Loss, destruction; Interruption |

### IT Staff Worksheet A4.3 Threat Trees

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  | (2.4) |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  | (3.2) |
| IT Staff |  | network |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | (2.2) |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

* (2.2) Concerned with monitoring system, including IoT cameras. These are on their own network.

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  | (1.1), (2.1)  (3.1), (3.2) |
| IT Staff |  | physical |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**Note**:

* (1.1) (2.1) (3.1) Concerned with the availability of the IT staff member.

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | viruses |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
| IT Staff |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | (1.2), (4.1) |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |

**Note**:

* (1.2) (4.1) Concerned with the general access and availability of an IT staff group in the company. The system of maintaining an IT staff is documented here as a “crash” if the IT staff is unavailable.

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | (2.3) |
| IT Staff |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  | (4.2) |
|  |  |  |  | interruption |  | (4.2) |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  | (2.2) |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  | (2.2) |

**Note**:

* (2.2) Concerned with IoT monitoring cameras.

### IT Staff Worksheet A5.1 Identify Key Classes of Components

|  |  |
| --- | --- |
| **IT Staff** | |
| **Class of Component** | **Rationale for Selection** |
| * Sickness | Sickness would mean IT Staff members would need to stay away from work. |
| * Injury | Injury would mean IT Staff members would need to stay away from work. If on the job, it could mean Swisher may be responsible. |
| * Death | Death would mean IT Staff members would need to stay away from work. If on the job, it could mean Swisher may be responsible. |
| * Leaving | Absence of IT Staff would mean Swisher will have no one to run the network and systems. |
| * Mistakes | Mistakes performed by IT Staff could have devastating effects on the company. |
| * Social Engineering | Humans are prone to social engineering attacks, and if the IT Staff is social engineered to give away credentials or grant access, many issues could occur. |
| * Others (list)   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

### IT Staff Worksheet A5.2 Identify Infrastructure Components to Examine

| **Class of Component** | **Selected Component/ IP Addresses/Host Names** | **Rationale** | **Approach** |
| --- | --- | --- | --- |
| System of interest | IT Staff | Only one IT Staff member in the IT Staff system of interest. She operates all IT tasks of Swisher’s. | Performance of pass/fail audits on specific components related to the IT Staff system of interest. |
| Sickness | General Sickness | Sickness would mean IT Staff members would need to stay away from work. | HR will test the impact of the IT Staff becoming sick.  1. Verify that there are backup staff members.  2. Verify that the IT Staff has sick days off.  3. Verify that there are medical supplies available in the building. |
| Injury | Physical Damage | Injury would mean IT Staff members would need to stay away from work. If on the job, it could mean Swisher may be responsible. | HR will test the impact of the IT Staff sustaining injury.  1. Verify that there are backup staff members.  2. Verify that there is a way for remote work to be done.  3. Verify that there is an injury reporting procedure in place. |
| Death | General Death | Death would mean IT Staff members would need to stay away from work. If on the job, it could mean Swisher may be responsible. | HR will test the impact of the IT Staff being deceased.  1. Verify that there are backup staff members.  2. Verify that there are documents related to death upon acceptance of the job.  3. Verify that there are opportunities to hire additional IT Staff members. |
| Leaving | Resignation | Absence of IT Staff would mean Swisher will have no one to run the network and systems. | HR will test the impact of the IT Staff resigning from the company.  1. Verify that there are backup staff members.  2. Verify that there is a document for non-disclosure of information.  3. Verify that there are opportunities to hire additional IT Staff members. |
| Mistakes | Error in Task | Mistakes performed by IT Staff could have devastating effects on the company. | HR will test the impact of the IT Staff causing mistakes in their work.  1. Verify that there are disciplinary actions in place.  2. Verify that additional training is available. |
| Social Engineering | All Individuals | Humans are prone to social engineering attacks, and if the IT Staff is social engineered to give away credentials or grant access, many issues could occur. | HR will test the vulnerability and impact of a social engineering attack against the IT Staff.  1. Verify that there is training in place to identify security threats such as social engineering.  2. Verify that the IT Staff is capable of identifying a social engineering attack through a simulation.  3. Verify that the IT Staff have methods to report a potential social engineering attack. |

### IT Staff Worksheet A6.1 Review Technology Vulnerabilities and Summarize Results

| **Asset: IT Staff** | | | |
| --- | --- | --- | --- |
| **Class** | **Selected Component/ IP Address/Host Name** | **Results** | **Vulnerability Summary** |
| Sickness | General Sickness | 1. Fail  2. Fail  3. Pass | - medium  - low |
| Injury | Physical Damage | 1. Fail  2. Fail  3. Pass | - medium  - low |
| Death | General Death | 1. Fail  2. Pass  3. Fail | - medium  - low |
| Leaving | Resignation | 1. Fail  2. Pass  3. Fail | - medium  - low |
| Mistakes | Error in Task | 1. Fail  2. Fail | - low  - low |
| Social  engineering | All Individuals | 1. Fail  2. Pass  3. Fail | - low  - medium |

|  |
| --- |
| **Actions and Recommendations for Addressing Technology Vulnerabilities** |
| **IT Staff** |
| General Sickness – The general sickness for IT staff has one medium and one low severity issue. The medium severity issue is that there is no backup IT staff if one person were to get sick. This could really hurt Swisher, because if an incident were to occur that requires an IT personnel, they would need to hire a third-party quickly that may not know their system processes. The low issue is that IT staff do not have sick days off. This could financially discourage the IT staff members, causing them to leave Swisher, leaving it staff-less for their IT needs. |
| Physical Damage – The physical damage for IT staff has one medium and one low severity issue. The medium severity is that there is no backup IT staff if one person were to get sick, and has the same rationale as in “General Sickness.” The low issue is that there is no way for remote work to be done. This really puts Swisher at risk if their IT staff were to get an injury that could keep them out of the office for an extended period of time. |
| General Death – The general death for IT staff has one medium and one low severity issue. The medium severity is that there is no backup IT staff if one person were to get sick, and has the same rationale as in “General Sickness.” The low severity issue is that there are no immediate opportunities for Swisher to hire new IT staff members. Not having an IT staff member on-site will require Swisher to hire a third-party quickly that may not know their system processes. |
| Resignation – The resignation for IT staff has one medium and one low severity issue. The medium severity is that there is no backup IT staff if one person were to get sick, and has the same rationale as in “General Sickness.” The low severity issue is that there are no immediate opportunities for Swisher to hire new IT staff members. Not having an IT staff member on-site will require Swisher to hire a third-party quickly that may not know their system processes. |
| Error in Task – The error in task for IT staff has two low severity issues. The two low severity issues are that there is no disciplinary action for mistakes and that there is no training available to prevent mistakes. Disciplinary action for consistent mistakes should exist as so to curb the possibility of it occurring again. This is the same idea behind a training program, which Swisher does not have in place. |
| All Individuals – All individuals are capable of social engineering the IT staff, and contains one medium and one low severity issue. The medium severity issue is that the IT staff does not have an outlet where they can report a potential engineering attack. One of the most crucial ways to prevent a social engineering attack to raise awareness that there may be a person who is doing it. The low severity issue is that there is no training in place for IT staff, or any staff at that, to identity social engineering attacks. Education is the best place to begin, as it teaches individuals what a social engineering attack looks like, so they can spot one when it is happening to someone or themselves. |

### IT Staff Worksheet A7.1 Identify the Impact of Threats to Critical Assets

| **IT Staff** | | | |
| --- | --- | --- | --- |
| **Impacts to the Organization** | | | |
| **Outcome** | **Consider** | **Impact Descriptions** | **Values** |
| **Disclosure** | * How could the organization’s reputation be affected if this asset were disclosed? * How could customer confidence be affected if this asset were disclosed? * How could the health of customers be affected if this asset were disclosed? * How could employee productivity be affected if this asset were disclosed? * How would other users of this asset be affected if this asset were disclosed? * What fines, legal penalties, or lawsuits could be imposed as a result of disclosure of this asset? * How could the organization be affected financially if this asset were disclosed? * What other impacts could occur if this asset were disclosed? For example: * ethical considerations * other legal/financial impacts | * If IT staff were to be disclosed, clients as well as vendors may view Swisher’s security training to be deficient, and may not be able to protect their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the IT staff were disclosed because it means that Swisher does not have the means to train their staff. * Disclosure of the IT staff has no ill effect on customer’s health. * Disclosure of the IT staff may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the IT staff from overworking. * There are no other users of the IT staff other than the staff at Swisher. * Disclosure of the IT staff at Swisher’s may breach OSHA laws. * Disclosure of the IT staff will have no financial impact on Swisher. * All considerations to disclosure of impacts have been made in relation to Swisher’s IT staff. |  |
| **Modification** | * How could the organization’s reputation be affected if this asset were modified? * How could customer confidence be affected if this asset were modified? * How could the health of customers be affected if this asset were modified? * How could employee productivity be affected if this asset were modified? * How would other users of this asset be affected if this asset were modified? * What fines, legal penalties, or lawsuits could be imposed as a result of modification of this asset? * How could the organization be affected financially if this asset were modified? * What other impacts could occur if this asset were modified? For example: * ethical considerations * other legal/financial impacts | * If IT staff were to be modified, clients as well as vendors may view Swisher’s security training to be deficient, and may not be able to protect their information that may be in the company. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the IT staff were modified because it means that Swisher does not have the means to train their staff. * Modification of the IT staff has no ill effect on customer’s health. * Modification of the IT staff may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the IT staff from overworking. * There are no other users of the IT staff other than the staff at Swisher. * Modification of the IT staff at Swisher’s does not breach any laws or regulations and not subject to legal penalties. * Modification of the IT staff may have financial impacts on Swisher if they are being social engineered. * All considerations to modification of impacts have been made in relation to Swisher’s IT staff. |  |
| **Destruction/Loss** | * How could the organization’s reputation be affected if this asset were destroyed, lost, or unavailable? * How could customer confidence be affected if this asset were destroyed, lost, or unavailable? * How could the health of customers be affected if this asset were destroyed, lost, or unavailable? * How could employee productivity be affected if this asset were destroyed, lost, or unavailable? * How would other users of this asset be affected if this asset were destroyed, lost, or unavailable? * What fines, legal penalties, or lawsuits could be imposed as a result of destruction/loss of this asset? * How could the organization be affected financially if this asset were destroyed, lost, or unavailable? * What other impacts could occur if this asset were destroyed, lost, or unavailable? For example: * ethical considerations * other legal/financial impacts | * If IT staff were to be destroyed/lost, clients as well as vendors may view Swisher’s HR policies to be deficient, and may not be able to support their staff. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the IT staff were destroyed/lost because it means that Swisher does not have the means to support their staff. * Destruction/loss of the IT staff has no ill effect on customer’s health. * Destruction/loss of the IT staff may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the IT staff from overworking. * There are no other users of the IT staff other than the staff at Swisher. * Destruction/loss of the IT staff at Swisher’s may breach OSHA laws. * Destruction/loss of the IT staff may have financial impacts on Swisher if they cannot get replacements fast. * All considerations to destruction/loss of impacts have been made in relation to Swisher’s IT staff. |  |
| **Interruption** | * How could the organization’s reputation be affected if access to this asset were unavailable? * How could customer confidence be affected if access to this asset were unavailable? * How could the health of customers be affected if access to this asset were unavailable? * How could employee productivity be affected if access to this asset were unavailable? * How would other users of this asset be affected if access to this asset were unavailable? * What fines, legal penalties, or lawsuits could be imposed as a result of unavailability of this asset? * How could the organization be affected financially if access to this asset were unavailable? * What other impacts could occur if access to this asset were unavailable? For example: * ethical considerations * other legal/financial impacts | * If IT Staff were to be unavailable, clients as well as vendors may view Swisher’s HR policies to be deficient, and may not be able to support their staff. Loss of business can be due to clients and vendors not supporting Swisher anymore. * Customer confidence would drop significantly if the IT staff were unavailable because it means that Swisher does not have the means to support their staff. * Unavailability of the IT staff has no ill effect on customer’s health. * Unavailability of the IT staff may reduce employee morale and faith in Swisher’s ability to keep information assets secure. This can lead to reduced productivity. Alternatively, the management could use it to motivate employees to increase their productivity towards helping keep the IT staff from overworking. * There are no other users of the IT staff other than the staff at Swisher. * Unavailability of the IT staff at Swisher’s does not breach any laws or regulations and not subject to legal penalties. * Unavailability of the IT staff may have financial impacts on Swisher as no one is available to keep their systems operating. * All considerations to unavailability of impacts have been made in relation to Swisher’s IT staff. |  |

### IT Staff Worksheet A7.2 Create Risk Evaluation Criteria

| IT Staff Evaluation Criteria | | | |
| --- | --- | --- | --- |
| **Impact Area** | **High** | **Medium** | **Low** |
| Reputation/ Customer Confidence | * Reputation irrevocably destroyed or damaged * More than 30% drop in customers due to loss of confidence | * Reputation damaged; some effort and expense required to recover * 10 to 30% drop in customers due to loss of confidence * Customer goes to competitor | * Reputation minimally affected; little or no effort or expense required to recover * Less than 10% drop in customers due to loss of confidence |
| Life/ Health of Customers | * Loss of customer life * Permanent impairment of one or more significant aspects of customer’s health (e.g., loss of use of one or more limbs, blindness, brain damage) * Safety violated | * Customer life threatened but recoverable with additional treatment * Temporary or recoverable impairment of customer’s health (e.g., recovering use of limbs through physical therapy) * Safety affected | * No loss or significant threat to customer life * Minimal, immediately treatable degradation in customer heath with recovery within four days * Safety questioned |
| Productivity | * Staff unable to perform critical job aspects for three or more days * 40% or more increase in work hours required of at least 10% of general staff for > three days * Irrecoverable loss of server data | * Staff work increased by 10-40% for one day * Increases in general staff work of 10-40% for one day * Inefficient continuity of availability; delays while recovering misplaced information | * Staff inconvenienced for less than a day but no measurable increase in work effort occurs * General staff inconvenienced for less than a day but no measurable increase in work effort occurs |
| Fines/ Legal Penalties | * Fines of greater than $100,000 levied * One or more non-frivolous lawsuits of more than $3,000,000 filed by customers * Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices | * Fines of $10,000 to $100,000 levied * One or more non-frivolous lawsuits between $250,000 and $3,000,000 filed by customers * Government or other investigative organization requests information or records (low-profile) | * No fine or a fine of less than $10,000 levied * Lawsuit of less than $250,000 or frivolous lawsuit (95% sure it can be defeated) filed by customer * No queries from government or other investigative organizations |
| Finances | * Yearly operational costs up 15% * 20% yearly revenue loss * One-time financial cost > $1M * Uncorrectable errors in funding and personnel | * Yearly operational costs up 2-15% * 5-20% yearly revenue loss * One-time financial cost of $25K to $1M * Partially correctable errors in funding and personnel | * Increase of less than 2% in operating costs * <5% yearly revenue loss * One-time financial cost of <$25K * Inconvenient but correctable errors in funding and personnel |

### IT Staff Worksheet A7.3 Evaluate the Impacts of Threats to Critical Assets

**Human Actors Using Network Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Medium |
|  |  |  |  |  |  | accidental |  | modification |  | Medium |
|  |  |  |  |  |  |  |  | loss, destruction |  | High |
|  |  |  |  |  |  |  |  | interruption |  | Medium |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Medium |
|  |  |  |  |  |  | deliberate |  | modification |  | Medium |
|  |  |  |  |  |  |  |  | loss, destruction |  | High |
|  |  |  |  |  |  |  |  | interruption |  | Medium |
| IT Staff |  | network |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Medium |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  | Medium |
|  |  |  |  |  |  | deliberate |  | modification |  | Medium |
|  |  |  |  |  |  |  |  | loss, destruction |  | High |
|  |  |  |  |  |  |  |  | interruption |  | Medium |

**Human Actors Using Physical Access**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACCESS |  | ACTOR |  | MOTIVE |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | inside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  | Medium |
| IT Staff |  | physical |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | accidental |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |
|  |  |  |  | outside |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | disclosure |  |  |
|  |  |  |  |  |  | deliberate |  | modification |  |  |
|  |  |  |  |  |  |  |  | loss, destruction |  |  |
|  |  |  |  |  |  |  |  | interruption |  |  |

**System Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | software defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | viruses |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
| IT Staff |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | system crashes |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | Medium |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | hardware defects |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |

**Other Problems**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ASSET |  | ACTOR |  | OUTCOME |  | IMPACT |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | power supply problems |  | modification |  |  |
|  |  |  |  | loss, destruction |  |  |
|  |  |  |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | telecommunications |  | modification |  |  |
|  |  | problems or unavailability |  | loss, destruction |  |  |
|  |  |  |  | interruption |  | Medium |
| IT Staff |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | third-party problems |  | modification |  |  |
|  |  | or unavailability of |  | loss, destruction |  |  |
|  |  | third-party systems |  | interruption |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  |  |
|  |  | natural disasters |  | modification |  |  |
|  |  | (e.g., flood, fire, tornado) |  | loss, destruction |  | High |
|  |  |  |  | interruption |  | Medium |
|  |  |  |  |  |  |  |
|  |  |  |  | disclosure |  | Medium |
|  |  | physical configuration or |  | modification |  |  |
|  |  | arrangement of buildings, |  | loss, destruction |  |  |
|  |  | offices, or equipment |  | interruption |  | Medium |

# Process 8A

## Process W8A.1 Current Protection Strategy

| **Security Awareness and Training (SP1): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Staff members understand their security roles and responsibilities. This is documented and verified. | Yes | Yes | No | Yes |
| There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified. | Yes | Yes | Unclear | Yes |
| Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. | Unclear | Unclear | No | Yes |

| **Security Awareness and Training (SP1): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | All services, mechanisms, and technologies have adequate in-house support. Documentation is available to show that all staff know their security roles and responsibilities. | No security awareness, training, and reminders to staff can see security measures deteriorate over time. |
| Operational Area Management | All services, mechanisms, and technologies have adequate in-house support. Documentation is available to show that all staff know their security roles and responsibilities. | No security awareness, training, and reminders to staff can see security measures deteriorate over time. |
| Staff | N/A | Do not know their security roles and responsibilities. |
| IT Staff | All staff get security awareness training. | N/A |

| **Security Strategy (SP2): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| The organization’s business strategies routinely incorporate security considerations. | Yes | Unclear |  | Yes |
| Security strategies and policies take into consideration the organization’s business strategies and goals. | Yes | Unclear |  | Yes |
| Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization. | Yes | Unclear |  | Yes |

| **Security Strategy (SP2): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | We update our security policies regarding our business strategies and goals. | Staff do not concern themselves the security policies regarding business strategies and goals. |
| Operational Area Management | N/A | Unsure of what security policies that we have concerning our business strategies and goals. |
| Staff | N/A | N/A |
| IT Staff | We update our security policies regarding our business strategies and goals. | N/A |

| **Security Management (SP3): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Management allocates sufficient funds and resources to information security activities. | Yes | Unclear | Yes | No |
| Security roles and responsibilities are defined for all staff in the organization. | Yes | Yes | Unclear | Yes |
| The organization’s hiring and termination practices for staff take information security issues into account. | Yes | Unclear | Unclear | Yes |
| The organization manages information security risks, including   * assessing risks to information security * taking steps to mitigate information security risks | Yes | Unclear | No | Yes |
| Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments). | Unclear | Unclear |  | Yes |

| **Security Management (SP3): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | The company assess risks to information security and takes steps to mitigate them. | Staff do not know their roles and responsibilities. |
| Operational Area Management | Everyone knows their security roles and responsibilities. | N/A |
| Staff | N/A | Unsure of security roles and responsibilities. |
| IT Staff | Managers do a good job defining security roles and responsibilities of staff and the necessary steps to take to mitigate a possible security incident. | Not enough resources allocated to information security activities. |

| **Security Policies and Regulations (SP4): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. | Yes | No | No | No |
| There is a documented process for management of security policies, including   * creation * administration (including periodic reviews and updates) * communication | Unclear | Unclear | Unclear | Yes |
| The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements. | No | Unclear |  | Yes |
| The organization uniformly enforces its security policies. | Yes | Yes | No | Yes |

| **Security Policies and Regulations (SP4): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | We have security policies in place that we update regularly and enforce them when required to. | Staff do not seem aware of the security policies and regulations. |
| Operational Area Management | We have security policies in place that we enforce when required to. | The security policies are not updated regularly. |
| Staff | N/A | There are no security policies in place to our knowledge. |
| IT Staff | N/A | We do not update the security policies and are using outdated ones. The staff are not made aware of the policies that do exist. |

| **Collaborative Security Management (SP5): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including   * protecting information belonging to other organizations * understanding the security policies and procedures of external organizations * ending access to information by terminated external personnel | Yes | Unclear | No | Yes |
| The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements. | Yes | Unclear |  | Yes |

| **Collaborative Security Management (S5): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | We have policies and procedures in place to protect our information assets when dealing with external organizations. | The operational managers should be aware of these policies too but they do not pay much attention to them. |
| Operational Area Management | N/A | N/A |
| Staff | N/A | N/A |
| IT Staff | We have policies and procedures in place to protect our information assets when dealing with external organizations. | The operational managers should be aware of these policies too but they do not pay much attention to them. |

| **Contingency Planning/Disaster Recovery (SP6): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| An analysis of operations, applications, and data criticality has been performed. | Unclear | Yes |  | Unclear |
| The organization has documented, reviewed, and tested   * business continuity or emergency operation plans * disaster recovery plan(s) * contingency plan(s) for responding to emergencies | Yes | Unclear |  | Yes |
| The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls. | Yes | Yes |  | Yes |
| All staff are   * aware of the contingency, disaster recovery, and business continuity plans * understand and are able to carry out their responsibilities | Unclear | No | Unclear | Yes |

| **Contingency Planning/Disaster Recovery (SP6): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | We have documented contingency plans for our information assets in the event that there is a disaster. | The staff do not seem to know their responsibilities associated with the contingency plans. |
| Operational Area Management | We have documented contingency plans for our information assets in the event that there is a disaster. | The staff do not know their responsibilities associated with the contingency plans. |
| Staff | N/A | Not sure of our responsibilities during a contingency plan. |
| IT Staff | We have documented contingency plans for our information assets in the event that there is a disaster. | N/A |

## Process W8A.2 Current Operational Practices

| **Physical Security Plans and Procedures (OP1.1): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested. | Yes | Yes | Unclear | Yes |
| There are documented policies and procedures for managing visitors. | No | Yes | Unclear | Yes |
| There are documented policies and procedures for physical control of hardware and software. | Yes | Yes | Yes | Yes |

| **Physical Security Plans and Procedures (OP1.1): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | We have physical security plans for safeguarding the building and its premise. We also have them for our hardware and software controllers. | N/A |
| Operational Area Management | We have physical security plans for safeguarding the building and its premise. We also have them for our hardware and software controllers. | N/A |
| Staff | There are policies concerning hardware and software controllers. | Too many people going into the lab. |
| IT Staff | We have physical security plans for safeguarding the building and its premise. We also have them for our hardware and software controllers. | Too many people going into the lab. |

| **Physical Access Control (OP1.2): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media. | Yes | Unclear | No | Yes |
| Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access. | Unclear | Yes | No | Yes |

| **Physical Access Control (OP1.2): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | We have policies in place regarding physical access to work areas and hardware. | N/A |
| Operational Area Management | Hardware components are physically safeguarded. | Too many people in the lab. |
| Staff | N/A | Too many people in the lab. |
| IT Staff | We have policies in place regarding physical access to work areas and hardware. Hardware components are physically safeguarded. | Too many people in the lab. |

| **Monitoring and Auditing Physical Security (OP1.3): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Maintenance records are kept to document the repairs and modifications of a facility’s physical components. |  |  |  | Yes |
| An individual’s or group’s actions, with respect to all physically controlled media, can be accounted for. |  |  |  | No |
| Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed. |  | Unclear |  | Yes |

| **Monitoring and Auditing Physical Security (OP1.3): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | N/A | N/A |
| Operational Area Management | N/A | People may try to break into the company’s property and steal materials or get hurt. |
| Staff | N/A | N/A |
| IT Staff | We have IoT cameras that are on their own network monitoring key locations. | Hard to located staff when they log in with other’s credentials. |

| **System and Network Management (OP2.1): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| There are documented and tested security plan(s) for safeguarding the systems and networks. | Yes | Unclear |  | Yes |
| Sensitive information is protected by secure storage (e.g., backups stored off site, discard process for sensitive information). |  |  |  | Yes |
| The integrity of installed software is regularly verified. |  |  |  | Yes |
| All systems are up to date with respect to revisions, patches, and recommendations in security advisories. |  |  |  | Yes |
| There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans. | No | Unclear | No | Yes |
| Changes to IT hardware and software are planned, controlled, and documented. |  |  |  | Yes |
| IT staff members follow procedures when issuing, changing, and terminating users’ passwords, accounts, and privileges.   * Unique user identification is required for all information system users, including third-party users. * Default accounts and default passwords have been removed from systems. |  |  |  | Yes |
| Only necessary services are running on systems – all unnecessary services have been removed. |  |  |  | Yes |

| **System and Network Management (OP2.1): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | We have security plans in place to protect the system and networks. | We do not have backups for our software and data. |
| Operational Area Management | N/A | We do not have backups for our software and data. |
| Staff | N/A | N/A |
| IT Staff | We have security plans in place to protect the system and networks. | N/A |

| **System Administration Tools (OP2.2): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced. |  |  |  | Unclear |

| **System Administration Tools (OP2.2): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | N/A | N/A |
| Operational Area Management | N/A | N/A |
| Staff | N/A | N/A |
| IT Staff | N/A | Not sure if the mechanisms for securing our system are updated regularly. |

| **Monitoring and Auditing IT Security (OP2.3): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure. |  |  |  | Yes |
| Firewall and other security components are periodically audited for compliance with policy. |  |  |  | Yes |

| **Monitoring and Auditing IT Security (OP2.3): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | N/A | N/A |
| Operational Area Management | N/A | N/A |
| Staff | N/A | N/A |
| IT Staff | There are monitoring tools in place for the system as well as firewalls. | N/A |

| **Authentication and Authorization (OP2.4): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections. |  |  |  | Yes |
| There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups. | Yes | Yes |  | Yes |
| Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified. |  |  |  | No |

| **Authentication and Authorization (OP2.4): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | We have policies and procedures in place that prevent terminated employees from accessing information. | N/A |
| Operational Area Management | We have policies and procedures in place that prevent terminated employees from accessing information. | N/A |
| Staff | N/A | N/A |
| IT Staff | We have access controls in place for authentication and authorization of individuals. | There are no mechanisms in place to ensure sensitive data hasn’t been accessed, altered, or destroyed in an unauthorized manner. |

| **Vulnerability Management (OP2.5): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| There is a documented set of procedures for managing vulnerabilities, including   * selecting vulnerability evaluation tools, checklists, and scripts * keeping up to date with known vulnerability types and attack methods * reviewing sources of information on vulnerability announcements, security alerts, and notices * identifying infrastructure components to be evaluated * scheduling of vulnerability evaluations * interpreting and responding to the results * maintaining secure storage and disposition of vulnerability data |  |  |  | Yes |
| Vulnerability management procedures are followed and are periodically reviewed and updated. |  |  |  | No |
| Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified. |  |  |  | No |

| **Vulnerability Management (OP2.5): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | N/A | N/A |
| Operational Area Management | N/A | N/A |
| Staff | N/A | N/A |
| IT Staff | We have procedures for managing vulnerabilities. | Vulnerability management and assessment is rarely tested and updated. |

| **Encryption (OP2.6): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology). |  |  |  | Yes |
| Encrypted protocols are used when remotely managing systems, routers, and firewalls. |  |  |  | Yes |

| **Encryption (OP2.6): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | N/A | N/A |
| Operational Area Management | N/A | N/A |
| Staff | N/A | N/A |
| IT Staff | We have encryption tools in place to protect our information assets. | N/A |

| **Security Architecture and Design (OP2.7): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| System architecture and design for new and revised systems include considerations for   * security strategies, policies, and procedures * history of security compromises * results of security risk assessments |  |  |  | Yes |
| The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology. |  |  |  | Yes |

| **Security Architecture and Design (OP2.7): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | N/A | N/A |
| Operational Area Management | N/A | N/A |
| Staff | N/A | N/A |
| IT Staff | All new designs and architectures for our security system go through careful security consideration. | N/A |

| **Incident Management (OP3.1): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations. | Yes | Unclear | Yes | Yes |
| Incident management procedures are periodically tested, verified, and updated. | Yes | Unclear | No | Yes |
| There are documented policies and procedures for working with law enforcement agencies. | Yes | Unclear | No | Yes |

| **Incident Management (OP3.1): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | We have incident procedures in place and they are tested and updated regularly. | Operational managers do not know about the incident procedures in place. |
| Operational Area Management | N/A | N/A |
| Staff | There are incident procedures in place. | N/A |
| IT Staff | We have incident procedures in place and they are tested and updated regularly. | Operational managers do not know about the incident procedures in place. |

| **General Staff Practices (OP3.2): Survey Results** | | | | |
| --- | --- | --- | --- | --- |
| **Survey Statement** | **Senior Managers** | **Operational Area Managers** | **Staff** | **IT Staff** |
| Staff members follow good security practice, such as   * securing information for which they are responsible * not divulging sensitive information to others (resistance to social engineering) * having adequate ability to use information technology hardware and software * using good password practices * understanding and following security policies and regulations * recognizing and reporting incidents | No | Unclear | Unclear | Yes |
| All staff at all levels of responsibility implement their assigned roles and responsibility for information security. | Yes | Unclear | No | No |
| There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides. | Unclear | Unclear | No | No |

| **General Staff Practices (OP3.2): Contextual Information** | | |
| --- | --- | --- |
| **Organizational Level** | **Protection Strategy Practices** | **Organizational Vulnerabilities** |
| Senior Management | N/A | Have no idea if the staff know what they are required to do in terms of securing information assets. |
| Operational Area Management | N/A | Have no idea if the staff know what they are required to do in terms of securing information assets. |
| Staff | N/A | No idea what we’re supposed to do in terms of protecting information assets. |
| IT Staff | Staff have good security practices. | Staff do not understand their roles and responsibilities for securing information assets. |

## Process W8A.3 Protection Strategy for Strategic Practices

|  |  |
| --- | --- |
| **Protection Strategy for Strategic Practices**  **Security Awareness and Training (SP1)** | |
| **Questions to Consider** | **Strategies** |
| * What can you do to maintain or improve the level of information security training that all staff members receive (consider awareness training as well as technology-related training)? * Does your organization have adequate in-house expertise for all supported technologies? What can you do to improve your staff’s technology expertise? * What can you do to ensure that all staff members understand their security roles and responsibilities? | * Improving our awareness campaign by creating posters and popup banners on the staff workstations reminding them of the policies we have in place. * There is plenty of in-house training at Swisher’s. The best way to improve staff expertise is to produce an awareness campaign. * A survey can be distributed to every staff at the end of 3 months to ensure that they understand their security roles and responsibilities. |
| **Issues:** No issues. | |

|  |  |
| --- | --- |
| **Protection Strategy for Strategic Practices**  **Security Strategy (SP2)** | |
| **Questions to Consider** | **Strategies** |
| * Are security issues incorporated into your organization’s business strategy? What can you do to improve the way in which security issues are integrated with your organization’s business strategy? * Are business issues incorporated into your organization’s security strategy? What can you do to improve the way in which business issues are integrated with your organization’s security strategy? * What can you do to improve the way in which security strategies, goals, and objectives are documented and communicated to the organization? | * Yes. Swisher does an amazing job already with incorporating security issues related to the business strategy and need no further improvement at the moment. * Yes. Swisher does an amazing job already with incorporating security issues related to the business strategy and need no further improvement at the moment. * Additional training for operational managers. |
| **Issues:** No issues. | |

|  |  |
| --- | --- |
| **Protection Strategy for Strategic Practices**  **Security Management (SP3)** | |
| **Questions to Consider** | **Strategies** |
| * Does management allocate sufficient funds and resources to information security activities? What level of funding for information security activities is appropriate for your organization? * What can you do to ensure that security roles and responsibilities are defined for all staff in your organization? * Do your organization’s hiring and retention practices take information security issues into account (also applies to contractors and vendors)? What could you do to improve your organization’s hiring and retention practices? * What can you do to improve the way in which your organization manages its information security risk? * What can you do to improve the in which security-related information is communicated to your organization’s management? | * No. The IT staff is the group who is in charge of developing information security activities and they are not getting enough funds. Swisher should be spending approximately 10% of its budget on security. * Improved training and awareness for all staff. The hiring and retention practices do take information security issues into consideration. Having all staff sign a non-disclosure agreement. * Increased training and awareness campaign for all management and staff. * By having the managers go into training to be able to read reports regarding security related information. |
| **Issues:** No issues. | |

|  |  |
| --- | --- |
| **Protection Strategy for Strategic Practices**  **Security Policies and Regulations (SP4)** | |
| **Questions to Consider** | **Strategies** |
| * What can you do to ensure that your organization has a comprehensive set of documented, current security policies? * What can you do to improve the way in which your organization creates, updates, and communicates security policies? * Does your organization have procedures to ensure compliance with laws and regulations affecting security? What can you do to improve how well your organization complies with laws and regulations affecting security? * What can you do to ensure that your organization uniformly enforces its security policies? | * By having either the IT staff create one or bring in a third-party group that specializes in creating security policies. * By having defined times in which the policies must be updated. Yes, Swisher has procedures to ensure compliance with the laws and regulations affecting security. This can be improved by training and raising awareness in staff. * By ensuring all employees understand the security policies. |
| **Issues:** No issues. | |

|  |  |
| --- | --- |
| **Protection Strategy for Strategic Practices**  **Collaborative Security Management (SP5)** | |
| **Questions to Consider** | **Strategies** |
| * Does your organization have policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners)? What can your organization do to improve the way in which it protects information when working with external organizations? * What can your organization do to improve the way in which it verifies that external organizations are taking proper steps to protect critical information and systems? * What can your organization do to improve the way in which it verifies that outsourced security services, mechanisms, and technologies meet its needs and requirements? | * Yes. Swisher does an amazing job already with security issues related to the external organizations and need no further improvement at the moment. * By ensuring external organizations know our policies as well as having documentation to be required when dealing with critical information systems. * By testing the security services in a virtual machine. |
| **Issues:** No issues. | |

|  |  |
| --- | --- |
| **Protection Strategy for Strategic Practices**  **Contingency Planning/Disaster Recovery (SP6)** | |
| **Questions to Consider** | **Strategies** |
| * Does your organization have a defined business continuity plan? Has the business continuity plan been tested? What can you do to ensure that your organization has a defined and tested business continuity plan? * Does your organization have a defined disaster recovery plan? Has the disaster recovery plan been tested? What can you do to ensure that your organization has a defined and tested disaster recovery plan? * What can you do to ensure that staff members are aware of and understand your organization’s business continuity and disaster recovery plans? | * Yes, Swisher has a business continuity plan that has been tested, and is updated regularly. * Yes, Swisher has a disaster recovery plan that has been tested, and is updated regularly. * By providing simulations of the business continuity plan and disaster recovery plans. |
| **Issues:** No issues | |

## Process W8A.4 Protection Strategy for Operational Practices

|  |  |
| --- | --- |
| **Protection Strategy for Operational Practices**  **Physical Security (OP1)** | |
| **Questions to Consider** | **Strategies** |
| * What training and education initiatives could help your organization maintain or improve its physical security practices? * What funding level is appropriate to support your organization’s physical security needs? * Are your policies and procedures sufficient for your organization’s physical security needs? How could they be improved? * Who has responsibility for physical security? Should anyone else be involved? * What other departments in your organization should be involved with physical security? * What external experts could help you with physical security? How will you communicate your requirements? How will you verify that your requirements were met? | * No additional training or education is necessary. * Physical security is combined into the 10% security budget that should be funding the IT staff’s endeavors. * No, there are too many unauthorized personnel in the lab. Having a documentation of who comes into the building as well as authorization badges. * There isn’t a singular person responsible for physical security. If anyone should be involved, it would be the site safety manager. * The IT staff should be involved with physical security as they know what information assets need physical security. * External security companies could help with physical security. We would mention critical infrastructure that needs to be secured and it will be tested through a simulation. |
| **Issues:** No issues | |

|  |  |
| --- | --- |
| **Protection Strategy for Operational Practices**  **Information Technology Security (OP2)** | |
| **Questions to Consider** | **Strategies** |
| * What training and education initiatives could help your organization maintain or improve its information technology security practices? * What funding level is appropriate to support your organization’s information technology security needs? * Are your policies and procedures sufficient for your organization’s information technology security needs? How could they be improved? * Who has responsibility for information technology security? Should anyone else be involved? * What other departments in your organization should be involved with information technology security? * What external experts could help you with information technology security? How will you communicate your requirements? How will you verify that your requirements were met? | * Possible third-party training on top of the in-house training. * Swisher should be spending approximately 10% of its budget on security. * Yes. Swisher does a good job with keeping policies and procedures appropriate for the information assets and need no further improvement at the moment. * The IT administrator is the sole person responsible for the information technology security. Additional IT staff would be helpful. * The senior managers should be involved so they understand the risks and can make decisions. * A penetration testing service could help find vulnerabilities inside the network and information systems. Critical assets will be of most importance and it will be tested in a simulation. |
| **Issues:** No issues. | |

|  |  |
| --- | --- |
| **Protection Strategy for Operational Practices**  **Staff Security (OP3)** | |
| **Questions to Consider** | **Strategies** |
| * What training and education initiatives could help your organization maintain or improve its staff security practices? * What funding level is appropriate to support your staff security needs? * Are your policies and procedures sufficient for your staff security needs? How could they be improved? * Who has responsibility for staff security? Should anyone else be involved? * What other departments in your organization should be involved with staff security? * What external experts could help you with staff security? How will you communicate your requirements? How will you verify that your requirements were met? | * Possible third-party training on top of the in-house training. * Swisher should be spending approximately 10% of its budget on security. * Yes. Swisher does a good job with keeping policies and procedures appropriate for the staff security and need no further improvement at the moment. * The IT administrator is the sole person responsible for the information technology security. Additional IT staff would be helpful. * The senior managers should be involved so they understand the risks and can make decisions. * A penetration testing service could help find vulnerabilities inside the staff. A test to social engineer the staff would be appropriate. |
| **Issues:** No issues. | |

## Process A8.3 Mitigation Plans

|  |  |
| --- | --- |
| **Mitigation Plan for Human Actors Using Network Access** | |
| **Questions** | **Actions** |
| What actions could you take to recognize or detect this threat type as it is occurring?  What actions could you take to resist or prevent this threat type from occurring?  What actions could you take to recover from this threat type if it occurs?  What other actions could you take to address this threat type?  How will you test or verify that this mitigation plan works and is effective? | * Swisher needs to develop a better training program as well as an awareness campaign that regularly reminds employees of their training. For the systems and data, that would mean understanding possible phishing scams, and for the IT staff, it would be recognizing social engineering attacks. * Having awareness training would mean the staff and IT staff are more likely to recognize these threat types if they come across one. Additional security measures such as software such as IDS and IPS can help protect the network. * Recovery would require a disaster recovery plan, which Swisher has. The training of staff in the recovery plan would be paramount in recovery if this threat type were to happen. Regular attendance of threat simulations that would require a disaster recovery plan will be administered so staff know their roles and responsibilities in the case of such a threat being prevalent. * Other actions to address this threat type is by verifying that all devices on the network is registered. Unregistered devices could be a person who connected to the network without permission. * By running a simulation before and after the mitigation plan has been administered. These will have to span different departments, as staff who were exposed to the initial simulation will be more aware naturally, of future simulations. Then metrics between the two will be compared, such as time from when the incident was first discovered, what was done when it was discovered, and what the staff member and managers do with the knowledge. |

|  |  |
| --- | --- |
| **Mitigation Plan for Human Actors Using Physical Access** | |
| **Questions** | **Actions** |
| What actions could you take to recognize or detect this threat type as it is occurring?  What actions could you take to resist or prevent this threat type from occurring?  What actions could you take to recover from this threat type if it occurs?  What other actions could you take to address this threat type?  How will you test or verify that this mitigation plan works and is effective? | * Swisher needs to develop a better training program as well as an awareness campaign that regularly reminds employees of their training. For the systems and data, that would mean understanding possible phishing scams, and for the IT staff, it would be recognizing social engineering attacks. * Having awareness training would mean the staff and IT staff are more likely to recognize these threat types if they come across one. Additional security measures such as software such as IDS and IPS can help protect the network. * Recovery would require a disaster recovery plan, which Swisher has. The training of staff in the recovery plan would be paramount in recovery if this threat type were to happen. Regular attendance of threat simulations that would require a disaster recovery plan will be administered so staff know their roles and responsibilities in the case of such a threat being prevalent. * Physical barriers around Swisher’s property could be added, or updated. The biggest factor here is to keep people outside of the property, which is where all the information assets are stored. Coming at it with a layered security approach, a sturdy fence would be the first line of defense. Then additional ones mentioned above, such as physical barriers to servers, routers, switches, etc. * By running a simulation before and after the mitigation plan has been administered. These will have to span different departments, as staff who were exposed to the initial simulation will be more aware naturally, of future simulations. Then metrics between the two will be compared, such as time from when the incident was first discovered, what was done when it was discovered, and what the staff member and managers do with the knowledge. |

|  |  |
| --- | --- |
| **Mitigation Plan for System Problems** | |
| **Questions** | **Actions** |
| What actions could you take to recognize or detect this threat type as it is occurring?  What actions could you take to resist or prevent this threat type from occurring?  What actions could you take to recover from this threat type if it occurs?  What other actions could you take to address this threat type?  How will you test or verify that this mitigation plan works and is effective? | * Swisher needs to develop a better training program as well as an awareness campaign that regularly reminds employees of their training. For all employees, this would mean understanding what actions to take if they notice such an issue. * Having awareness training would mean the staff and IT staff are more likely to recognize these threat types if they come across one. System problems include a wide range of threat types, so there is no one method to securing it. One method for hardware is to ensure it is cleaned regularly to prevent dust buildup. * Recovery would require a disaster recovery plan, which Swisher has. The training of staff in the recovery plan would be paramount in recovery if this threat type were to happen. Regular attendance of threat simulations that would require a disaster recovery plan will be administered so staff know their roles and responsibilities in the case of such a threat being prevalent. * There are really no other methods to address software and hardware defects. System crashes are usually out of a person’s control, and can occur spontaneously. The one thing Swisher can do is to have an uninterruptable power supply (UPS), for their servers so when system crashes do happen, not everything shuts down. For viruses, training as mentioned above, but antiviruses on every workstation as well. * By running a simulation before and after the mitigation plan has been administered. These will have to span different departments, as staff who were exposed to the initial simulation will be more aware naturally, of future simulations. Then metrics between the two will be compared, such as time from when the incident was first discovered, what was done when it was discovered, and what the staff member and managers do with the knowledge. |

|  |  |
| --- | --- |
| **Mitigation Plan for Other Problems** | |
| **Questions** | **Actions** |
| What actions could you take to recognize or detect this threat type as it is occurring?  What actions could you take to resist or prevent this threat type from occurring?  What actions could you take to recover from this threat type if it occurs?  What other actions could you take to address this threat type?  How will you test or verify that this mitigation plan works and is effective? | * Swisher needs to develop a better training program as well as an awareness campaign that regularly reminds employees of their training. For all employees, this would mean understanding what actions to take if they notice such an issue. * Having awareness training would mean the staff and IT staff are more likely to recognize these threat types if they come across one. In addition to training, for such threats such as a natural disaster that would require a contingency plan, staff will attend regular simulations so they understand their roles and responsibilities during such an event. * Recovery would require a disaster recovery plan, which Swisher has. The training of staff in the recovery plan would be paramount in recovery if this threat type were to happen. Regular attendance of threat simulations that would require a disaster recovery plan will be administered so staff know their roles and responsibilities in the case of such a threat being prevalent. * The power supply problem can be solved with a UPS. With telecommunication problems, Swisher should ensure that they have a backup IPS that can provide services if one IPS goes down. Dealing with third-party should mean that they have to adhere to Swisher’s information security policies. * By running a simulation before and after the mitigation plan has been administered. These will have to span different departments, as staff who were exposed to the initial simulation will be more aware naturally, of future simulations. Then metrics between the two will be compared, such as time from when the incident was first discovered, what was done when it was discovered, and what the staff member and managers do with the knowledge. |

## Process W8A.5 Action List

| **Action Item(s)** | **Information** |
| --- | --- |
| * Create an access control list that only allows authorized personnel’s credentials to grant access to Swisher’s servers only. * Create awareness campaign for personnel to check that there no additional devices attached to a workstation before and after use. * Download VeraCrypt onto every workstation and create a training program to teach staff on how to encrypt critical information. * Verify all devices on the network are registered. | Responsibility: IT Staff  Completion date: Within 30 days  Required management actions: Address budgeting for awareness campaign. |
| * Develop a badge that would allow Swisher to identify employees as well as grant employees access based on their badge credentials. * Develop an information awareness campaign concerned with best security practices for staff. | Responsibility: IT Staff and Administrative Managers  Completion date: Within 60 days  Required management actions: Address budgeting for awareness campaign and development of employee badges. |
| * Make purchases of physical containers with locks that the servers, NAS, routers and switches can be stored in to prevent physical tampering. * Distribute more IoT monitoring cameras, specifically to mission critical assets as well as the perimeters of the property, which is concerned with physical security. * Purchase and install an IDS and IPS on the network. * Purchase and use a UPS for keeping servers running in case of an electrical issue. | Responsibility: IT Staff and Administrative Managers  Completion date: Within 90 days  Required management actions: Address budgeting for physical containers, IoT monitoring cameras, IDS/IPS software, and a UPS. |
| * Hire additional IT staff to alleviate the pressures off of the IT administrator. * Hire a penetration testing service to test the information system vulnerabilities in Swisher’s network and systems. * Update the information system policies in regards to contingency planning, business strategies, and others. | Responsibility: IT Staff and Administrative Managers  Completion date: Within 180 days  Required management actions: Address budgeting for hiring additional IT staff as well as external penetration testing services. |
| * Have an external auditing service come and audit the information system to the policies that Swisher has in place. * Have an additional IPS supplier in the case of Internet failures on one supplier’s end. | Responsibility: IT Staff and Administrative Managers  Completion date: Within a year  Required management actions: Address budgeting for hiring an external auditing service. |

# References

**General Data Protection Regulation (GDPR)**

European Commission. (May 25, 2018). 2018 Reform of EU Data Protection Rules. URL: https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules\_en (visited on 04/14/2020).

**Privacy Act of 1974**

Department of Justice. (2015). Privacy Act of 1074. URL: https://www.justice.gov/opcl/privacy-act-1974 (visited on 04/14/2020).

**Operational Safety and Health Organization (OSHA)**

United States Department of Labor. (2019). Operational Safety and Health Organization. URL: https://www.osha.gov/laws-regs (visited on 04/14/2020).