|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 1** | **Risk Measurement Criteria – Reputation and Customer Confidence** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Reputation* | A server failure for a few hours prevents customers from retrieving data from the software ABC Technologies provides. | A server failure for a 3 day period preventing customers from retrieving data from the software ABC Technologies provides. | A server failure for a week preventing customers from retrieving data from the software ABC Technologies provides. |
| *Customer Loss* | Less than 5 % reduction in customers due to loss of confidence | 5 to 25% reduction in customers due to loss of confidence | More than 25% reduction in customers due to loss of confidence |
| *Other: Lack of advertising* | The marketing campaign provides too much knowledge. | ABC Technologies uses irregular advertising. | No advertisement of ABC Technologies products other than the company website. |

**Low**

**A server failure for a few hours preventing customers from retrieving data from the software ABC Technologies provides.**

Having a server failure preventing customers from accessing data results in a loss of availability for the customers. The server failed due to a DDoS (Distributed Denial of Service) attack occurring. ABC Technologies recently changed internet providers and were not aware that the internet hosts didn’t include protection for this attack Cohen, G. (2021). The customers of ABC Technologies are also other businesses therefore they need to keep to deadlines and keep employees productive in order to keep their profit margins high. As it is only for a few hours customers may be annoyed however a few hours is not a long time. In addition the issues may only affect certain companies depending on their time zones. Customers could be lost due to this but only less than 5% as it is only for a few hours (Armony, Shimkin and Whitt, 2009). Less than 5% in customer loss has been chosen as the server is only down for a few hours, which may warrant some customers to want to cancel their subscription perhaps new customers are more likely to do this.

**Moderate**

**A server failure for a 3 day period preventing customers from retrieving data from the software ABC Technologies provides.**

Having a server failure preventing customers from accessing data results in a loss of availability for the customers. . The server is outdated resulting in components often failing and as the server is not hot swappable leaving the IT technicians to turn the server off for maintenance. On this occasion ABC Technologies did not have the correct part as it was something that didn’t often fail so the IT technicians were forces to wait 3 days for the part to arrive. The customers of ABC Technologies are also other businesses therefore they need to keep to deadlines and keep employees productive in order to keep their profit margins high. As it is 3 days it would have affected customers enough to want to cancel contracts with ABC Technologies. Companies around the globe will be affected by this and will lead to a medium customer loss of between 5% and 25%. New customers and customers who heavily depend on the software are the most likely to cancel their subscriptions. (Armony, Shimkin and Whitt, 2009). Although ABC Technologies the software activity side is not that large in comparison to the whole company and can be presumed the number of customers the software side of the company has is 50. This would mean that a moderate rate would be between 3 and 13 customers leaving.

**High**

**A server failure for a week preventing customers from retrieving data from the software ABC Technologies provides.**

When a server failure occurs it prevents customers from accessing data therefore resulting in a loss of availability for the customers. This occurred due to ABC Technologies buying a new server because the old one broke and soon after the new server stopped working due to power supply and hard drive issues (Cohen, G. 2021). As this was a new server the company ABC Technologies bought the server from were informed however due to shortages they were not able to source and fix the issue for 7 days. This resulted in customers becoming frustrated; customers of ABC Technologies are also other businesses therefore they need to keep to deadlines and keep employees productive in order to keep their profit margins high. As it is a week the customers cannot use the software for there will be a high reputation loss and customer loss as ABC Technologies is providing the service as should. Customer loss would be more than 25%. Given that it is presumed that the software side of the company has 50 customers this would be more than 13 customers leaving.

**Lack of advertising**

**Low**

**The marketing campaign provides too much knowledge.**

ABC Technologies uses too much product knowledge making potential customers question the sales team answer a bunch of question that otherwise customers would not be asking. For example the advert may say “best CRM” and not show any evidence of this causing questions to be asked about why that is the best (Tellis, G.J. 2003). This does bring potential customer to the organisation however the issue is that customers may only come to find out why it is the best CRM and be dissatisfied resulting in time of the sales rep being wasted.

**Moderate**

**ABC Technologies uses irregular advertising.**

ABC technologies may only push advertising for short periods of time when new products are released. This would bring in customers however it is only for a short period of time. This would result in potentially long periods where there is no advertising resulting in a significant drop of potential new customers when advertising stops (Tellis, G.J. 2003). ABC Technologies may do this due to budgets in which case they do not have many other options other than finding partnerships or finding places that allow for free advertising. The growth of the company will slow down due to advertising being stopped as it is likely less customers will be added to the software subscription. Having consistent advertising should result in a steady amount of potential customers asking for services from ABC Technologies.

**High**

**No advertisement of ABC Technologies products other than the company website.**

Having zero advertising is almost like shooting yourself in the foot. It is considered to be a bad business move as it restricts the company’s efforts to obtain new customers passively. Instead the marketing team is would have to cold call or go door to door to potential clients. Having some form of advertising like adverts on social media will allow more people to view the advert from a wider geographical area as well as potentially be targeted advertising (Keehler, J. 2022). Zero advertising will result in far less potential customers compared to advertising.

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 2** | **Risk Measurement Criteria – Financial** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Operating Costs* | Increase of less than 7% in yearly operating costs | Yearly operating costs increase by 7% to 15%. | Yearly operating costs increase by more than 15%. |
| *Revenue Loss* | Less than 5% yearly revenue loss | 5% to 15% yearly revenue loss | Greater than 15% yearly revenue loss |
| *One-Time Financial Loss* | One-time financial cost of less than £30000 | One-time financial cost of £30000 to £80000 | One-time financial cost greater than £80000 |
| *Other: Share Price* | Drop in price less than 3% in a quarter | Drop in price between 3% and 8% in a quarter | Drop in price more than 8% in a quarter |

**Operating costs**

**Low**

ABC Technologies is based in the United Kingdom thus has to follow The National Minimum Wage Act 1998 which sets out a minimum amount to pay workers per hour. This can cause up to a 7% operating cost increase just by keeping on the same employees before the national living wage increased. From 2021 to 2022 to minimum wage in the UK increased by 6.52% and rose from £8.91 to £9.50 (Commission, L.P. 2022).

**Moderate**

A 7% to 15% increase to operating costs can occur when there is noncompliance with policies and procedures within ABC Technologies (PECB 2011). This can result in disrupted services, such as hardware or software corruption, violations of physical access controls, and negative impacts on employee well-being. These disruptions can lead to reputational damage, audits, legal action, and penalties or fines. For example, a recent survey found that 63% of organisations have experienced at least one data breach due to hardware security vulnerability. Phishing is one of the main ways attackers try and gain information like login details from employees in order to gain sensitive information (Zhu, H. 2020).

**High**

Operating costs can go up more than 15% because of utilities due to an energy crisis. This would be for both gas and electricity however in ABC Technologies case it would be focusing on electricity. Electricity is used to power the building lights as well as all the hardware which in turn the company is heavily dependent on being as it has a software development department (Indeed, Editorial Team, (2021). On average the cost pence per kWh has risen from 21.2 to 27.75 which is a 32% increase (Yurday, E. 2023).

**Revenue Loss**

**Low**

If revenue loss is less than 5% for the year it can be considered that the company did not necessarily have a bad year and have maintained their performance. Revenue may not have increased because of lack of ability to gain new customers but were able to keep all existing customers. (Zhang, Q., Wang, J., Lu, A., Wang, S. and Ma, J. 2018)

**Moderate**

A revenue loss between 5% and 15 % is a moderate amount to lose over the year. In this scenario the company has a high turnover in employees therefore there is often confusion in projects because of lack of communication and skills. This slows down the projects, extending the deadlines as the code isn’t satisfactory. Employee training can help with getting employees competent in their roles and could help to reduce employee turnover.

**High**

Mass amount of customers decided to end their subscriptions with ABC Technologies. Losing a lot of customers can result in a very large amount of revenues being lost. With ABC Technologies offering three different plans: ABC Supreme (£3,995), ABC Pro (£495) and ABC (£295). It would only take 15 customers on the ABC Supreme plan to lose more than £15000. Assuming the revenue was £300000 the previous year that would be more than a 15% loss. (Deskera Content Team)

**One-Time Financial Loss**

**Low**

A one-time financial loss under £30000 for ABC Technologies is investing in new computer hardware to upgrade its technology infrastructure; not all the infrastructure would be upgraded here due to cost. ABC Technologies decided to make the investment in order to improve the efficiency and effectiveness of its operations. The new hardware included high-performance computers, servers, and networking equipment, as well as software licenses. The investment will help the company continue to deliver high-quality services to its clients and remain competitive in the market.

In 2017, there were a record number of data breaches, with 1,579 incidents reported by the Identity Theft Resource Center. This represented a 44.7% increase from the previous year. According to a study by the Ponemon Institute, nearly 70% of workers believe that their organizations existing security solutions are outdated and inadequate. This is a concern because older hardware and software may not have the latest security updates, making them more vulnerable to attacks. (Crook Z 2018).

A survey conducted by Microsoft found that more than 90% of people would consider taking their business elsewhere if a company used outdated technology, citing concerns about security, privacy, and user-friendly convenience (Crook Z 2018). Not only would the ABC Technologies benefit with faster and easier to use hardware and software but other companies are more likely to use ABC Technologies services.

**Moderate**

A financial cost between £30,000 and £80,000 could result from a data breach that occurs resulting in costs from hiring cyber security experts, informing affected customers, and implementing additional security measures (Gorecki A 2020). A data breach can be a significant issue for a company. Not only can it compromise the security and privacy of the company's customers, but it can also lead to financial losses for the company. In the event of a data breach, a company may incur costs associated with hiring cyber security experts to investigate and address the issue, informing affected customers about the breach and any necessary precautions, and implementing additional security measures to prevent future breaches. These costs can be significant and may impact the company's bottom line. It is important for companies to prioritisecyber security and take steps to prevent data breaches in order to protect their customers and their own financial well-being. ABC Technologies hardly has any security controls in place thus this scenario is very likely and may be considered a High impact area.

**High**

A significant software bug is discovered after the product has been released, requiring the company to spend significant resources to fix the issue and potentially offering compensation to affected customers (Callaghan, D. and O'Sullivan, C. 2005). Discovering a significant software bug after a product has been released can be a serious issue for a company. It can damage the company's reputation and lead to customer dissatisfaction. In order to fix the issue, the company may need to spend significant resources, including time and money, on development and testing efforts. Depending on the severity of the bug and the impact it has on customers, the company may also need to offer compensation, such as refunds or credits, to affected customers. The impact of this can easily cost ABC Technologies over £80,000. This can further impact the company's financial performance. It is important for ABC Technologies to prioritise quality control and thoroughly test their products before releasing them in order to minimise the risk of significant software bugs.

**Share Price**

Share prices are affected by the company’s reputation, profit margins and market dominance. It is fair to say most of the time a share price change over a quarter can determine how well a company has performed over that period of time (HADA, T., OLTEANU, E. and DOBRA, I.B., 2015).

**Low**

If ABC Technologies fails to release new software, it may lead to a decline in the company's stock price. This is because investors and analysts may view a lack of new software releases as a sign of a lack of innovation and growth potential. In the technology industry, where new products and services are constantly being developed and released, a company's ability to stay current and relevant is important in order to maintain market share and attract customers. If ABC Technologies is unable to release new software, it may be seen as falling behind its competitors and may lose ground in the market. This can lead to a decline in the company's stock price as investors lose confidence in the company's future prospects. In order to maintain a strong stock price, it is important for a company to continuously innovate and release new products and services. Over a period of a quarter this can affect the loss of share price by up to 3%.

**Moderate**

A price drop of between 3% and 8% is considered a moderate drop in terms of share price over a quarter. This would indicate that ABC Technologies is not growing and is starting to decline and would show in their profits. If ABC Technologies financial performance or outlook is weaker than expected, it may result in a decline in the company's share price. Financial performance refers to a company's financial results, such as its revenue, profits, and expenses, while outlook refers to the company's expected future financial performance. If a company's financial results fall short of expectations, or if analysts and investors have concerns about the company's future prospects, it may lead to a decrease in the company's share price. This may occur if the company experiences declining sales, increasing expenses, or other financial challenges that impact its profitability. A company's share price is influenced by investor sentiment and can be impacted by a range of factors, including the company's financial performance and outlook (Mahalingam, A., Coburn, A., Jung, C. J., Yeo, J. Z., Cooper. G., Evan, T. 2018). ABC technologies need to ensure that investors are happy with the performance of the company thus any bad publicity would drop the price share. Bad publicity such as poor finical growth for the quarter can be the reason for a 3% - 8% price drop.

**High**

A price drop of over 8% over a quarter can happen because of external factors outside of the company’s control that may impact the company's financial performance or investor sentiment. Examples of external events that may impact a company's share price include natural disasters, geopolitical tensions, and changes in government policies or regulations. For example, a natural disaster such as a hurricane or earthquake may disrupt a company's operations and supply chain, leading to a decline in its share price. Similarly, geopolitical tensions or changes in government policies may impact a company's ability to do business or may affect investor sentiment, leading to a decline in the company's share price (Mahalingam, A., Coburn, A., Jung, C. J., Yeo, J. Z., Cooper. G., Evan, T. 2018). External events can be difficult to predict and can have significant impacts on a company's financial performance and share price. As such, external events can be a source of uncertainty and risk for companies and may lead to a decline in the company's share price.

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 3** | **Risk Measurement Criteria – Productivity** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Staff Hours* | Staff work hours are increased by less than 2% for 1 to 2 day(s). | Staff work hours are increased between 2% and 4 % for 1 to 2 day(s). | Staff work hours are increased by greater than 4 % for 1 to 2 day(s). |
| *Other:* |  |  |  |
| *Other:* |  |  |  |
| *Other:* |  |  |  |

**Low**

Assuming an average work week for employees is 40 hours increasing the work hours by less than 2% would result in a maximum of 15 minutes per day. Although that is not a lot of time it can be enough time to plan and organise for the next day presuming that the following day is eventful (Caralli, R.A., Stevens, J.F., Young, L.R. and Wilson, W.R. 2007**).**

**Moderate**

Assuming an average work week for employees is 40 hours increasing the work hours between 2% and 4% would result in an increase of work hours of 16 to 32 minutes a day. Having an extra hour over a 2 day period allows for the CRM to have enough time to complete work on a project that is behind on its deadline, but not significantly behind.

**High**

Assuming an average work week for employees is 40 hours increasing the work hours by more than 4% would give at least 32 minutes per day extra. This would be done if project deadlines are behind or there has been a significant issue that needs resolving such as a new patch not working as planned therefore needs fixing or reverting back to the old one. Workers could also go on strike causing other employees to work extra hours (Tasya, M.A., Suwawi, D.D.J. and Utomo, R.G. 2022).

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 4** | **Risk Measurement Criteria – Safety and Health** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Life* | No loss or significant threat to customers’ or staff members’ lives | Customers’ or staff members’ lives are threatened, but they will recover after receiving medical treatment. | Loss of customers’ or staff members’ lives |
| *Health* | Minimal, immediately treatable degradation in customers’ or staff members’ health with recovery within four days | Temporary or recoverable impairment of customers’ or staff members’ health | Permanent impairment of significant aspects of customers’ or staff members’ health |
| *Safety* | Safety questioned | Safety affected | Safety violated |
| *Other:* |  |  |  |

**Low**

There has been an accident and someone has spilt water on the resin floor in the office. There is a wet floor sign present and an employee slips and falls as they do not see the sign as they were on their phone. They fall on their side and have a bit of pain but are fine after a day.

As the employee was on their phone they did not see the sign on the floor. Perhaps the sign should be placed in the middle of the wet patch to ensure employees see it in the future.

Safety is questioned however as there was a wet floor sign present there isn’t much more the workplace could do to warm employees. Therefore is no regulatory response (Whitman and Mattord, 2018).

ABC Technologies decided it was best to send an announcement reminding cleaning staff what is expected following HSE guidelines. Wet floors should be clearly marked with warning signs to alert people to the potential danger. Any spillages should be cleaned up immediately, and floor surfaces should be checked regularly to ensure they are dry and free of hazards. In the case of large spillages or persistent dampness, temporary barriers or floor mats may be necessary to prevent accidents. It is important to take all necessary precautions to prevent accidents and ensure the safety of all individuals in the area (Health and Safety Executive 2019a).

**Moderate**

Repetitive stress injuries (RSIs) can occur and can have the ability to impair an employee’s ability to perform at work. In the software activity team they are always typing and clicking using the computers which over time causes strain to muscles and tendons. If employees were not allowed breaks this can cause a concern as the employee may need medical treatment and be off work for more than 4 days; thus resulting in safety being affected.

The safety is affected there will be a regulatory response including an investigation which could incur up to £70 thousand in recovery and response costs (Marchese. T).

**High**

Faulty equipment is the number one reason for fires in the workplace thus it is important to regular review the condition of the equipment. This could be cause due to incorrect cabling, equipment overheating or past its life span. Fires are deadly due to the heat and the smoke that gets into lungs and prevents them from working correctly. There is no fire procedure in place at ABC Technologies, this goes against health and safety standards (Health and Safety Executive 2019). If ABC Technologies is found to have poor safety regulations they can face an unlimited fine and responsible persons up to two years in jail (UK GOV 2015).

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 5** | **Risk Measurement Criteria – Fines and Legal Penalties** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Fines* | Fines less than £100k are levied. | Fines between £100k and £250k are levied. | Fines greater than £250k are levied. |
| *Lawsuits* | Non-frivolous lawsuit or lawsuits less than £100k are filed against the organization, or frivolous lawsuit(s) are filed against the organization. | Non-frivolous lawsuit or lawsuits between £100k and £1M are filed against the organization. | Non-frivolous lawsuit or lawsuits greater than £1M are filed against the organization. |
| *Investigations* | No queries from government or other investigative organizations | Government or other investigative organization requests information or records (low profile). | Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices. |
| *Other:* |  |  |  |

**Fines**

**Low**

**Scenario:** A cyber-attack on the organisation that has taken down a server that allows users to access the software ABC Technologies provides.

ABC Technologies will have a contract that allows its customers to access its software whenever necessary. As the server is down this is not possible so a lawsuit can be field resulting in a penalty and/or lawsuit on a low scale. This would be no query from the government. (Ashton. L, 2020).

**Moderate**

**Scenario:** A cyber-attack on the organisation where the attacker has stolen debit/credit card details of users from the database.

The attacker was able to steal less that 10% of user’s card details and listed them on the dark web. Because it was a small amount it isn’t a high fine but is moderate, thus the lawsuit would also be on a moderate scale. The government will look into the organisation and request records from the organisation to see if the data is as sure as could be (Ashton. L, 2020, UK GOV, 2022).

**High**

**Scenario:** A cyber-attack occurs and the attacker finds that there is a database with no security and is able to steal all user information.

This would result in a high risk of a fine and a high scale lawsuit would occur because of the scale of the action. Clients could have been high profile and could have major backing from the government resulting. An in depth investigation would happen and likely very large fines may occur as the database wasn’t secured correctly (Suroso, J.S. and Fakhrozi, M.A. 2018, UK GOV 2022).

|  |  |  |  |
| --- | --- | --- | --- |
| **Allegro Worksheet 6** | **Risk Measurement Criteria – Third-parties** | | |
| **Impact Area** | **Low** | **Moderate** | **High** |
| *Third party suppliers* | Backlog | Batch of components are defective/ not correct. | Suppliers become insolvent |

**Third party suppliers**

**Low**

**Scenario**: ABC Technologies has a backlog of requests that the supplier hasn’t fulfilled yet. The supplier hasn’t fulfilled it as their servers are down therefore unable to add data to their database; 70% of service down time is caused by third party supplier (Lawrence, A. 2022). This stops employees of ABC Technologies to retrieve and update data in the third part database.

The cause’s issues with the software development team when they are trying to test the next patch as they are unable to retrieve user data to test. This causes delays in the project.

**Moderate**

A new batch of processers have been delivered to the office to help the software development team, however when the 1st five processor was installed it showed a fault code and is useable. Because of this the computers were unable to be upgraded and slowed production down as computers were out of use and the computers remain slow until supplier sends out new ones.

**High**

Third party suppliers have gone insolvent resulting in loss of databases and data within. ABC Technologies will have to find another supplier or host their own databases which both may be more expensive than before. Loss of data can result in inaccurate data being used and displayed to users as well as for testing purposes.

|  |  |  |
| --- | --- | --- |
| **Allegro Worksheet 7** | | **Impact Area Prioritization Worksheet** |
| **Priority** | **Impact Areas** | |
| 3 | **Reputation and Customer Confidence** | |
| 6 | **Financial** | |
| 2 | **Productivity** | |
| 4 | **Safety and Health** | |
| 5 | **Fines and Legal Penalties** | |
| 1 | **Third-parties** | |

**Financial**

Financial is the most important as the purpose of ABC Technologies is to provide a service and make profits over the year. If the company wasn’t able to have a good positive cash flow it would result in loss in productivity as employees wouldn’t have the correct equipment to do their job as well as employees leaving due not getting paid. In turn this will slow down the growth of the company and force the company to reduce the amount of project being undertaken. ABC Technologies wants to be back to being at the top in their market, it is at huge importance that they have sufficient amounts of money to be able to develop and buy what they need for (Calder & Watkins, 2010).

**Fines and legal penalties**

ABC Technologies can have fines coming their way between the moderate and high scale due to there being a high possibility of user details being leaked. This is because once an attacker gains access to the network they are able to find the user details without any security thus are very easy for them to steal the high value assets without much effort compared to if it was secured. This will lead to a high fine and repercussions and possibly affect the company’s perforce moving forward. Fines can also be given for not having regular audits and checking that all safety procedures are in place for example fire evacuation (UK GOV 2022).

**Safety and health**

It is important for a company to ensure all employees are kept safe and follow the best practices as these are the standard. Regulations for health and safety both protect the company as well as staff. Safety and health is placed as moderate concern as it is presumed that ABC Technologies has not performed checked to see if the new office building abides by these regulations are there could be some serious risks. These risks could include: gas leak, boiler not working so cannot heat the building, no procedures in case of floor or fire, access control for the building etc.

**Productivity**

It is presumed that ABC Technologies has an adequate amount of employees in their software activities department to keep up with demand so there is no need to increase productivity. Although there may be a need for the team to increase security straight away so may have to work a less than 2% extra over a 2 day period. It is not an immediate concern compared to other issues the company faces (Calder & Watkins, 2010).

**Reputation and customer confidence**

ABC Technologies have a lot of new competitor therefore need their company to have a strong reputation and customer confidence. Having good customer confidence and reputation allows the company to attract new clients as well as keep existing clients through performing well. It is unlikely the servers will consistently go down for prolonged periods of time denying customers access to the software for their business needs. Server going down also allows for a potential back door attack allowing attackers a way into the network and stealing assets (Ashton. L,2020).

**User Defined**

Third party suppliers are all very replaceable for ABC Technologies as the services are widely available if the suppliers didn’t meet the company’s needs. Currently ABC Technologies uses third party cloud providers and a remote login. Since ABC Technologies already had an existing cloud provider it will be less complex compared to updating a company not previously on the cloud thus on average will take 10 days to transfer provider (App Direct 2018).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Allegro Worksheet 8** | **Critical Information Asset Profile** | | | | |
| **(1) Critical Asset**  *What is the critical information asset?* | **(2) Rationale for Selection**  *Why is this information asset important to the organization?* | | | **(3) Description**  *What is the agreed-upon description of this information asset?* | |
| Product source code of software ABC Technologies use for their programs. | The product source code allows the company to create software that other companies can use and sell it to them as a subscription service. It is the main source of income through the software side of the company. | | | It is one of the most important assets in the company. The source code allows facilitates the acquisition of information, including customer data entry (name, contact information, availability, recreation). It allows a company to store, control and modify information, plan tasks, annotate notifications as well as several other functions (PECB 2011). | |
| **(4) Owner(s)**  *Who owns this information asset?* | | | | | |
| ABC Technologies owns the source code as employees sign a contract with a clause stating that the code written by them is owned by the company. | | | | | |
| **(5) Security Requirements**  *What are the security requirements for this information asset?* | | | | | |
| * **Confidentiality** | Only authorized personnel can view this information asset, as follows: | | **Members of the software activity.**  **CEO Sabrina Senat** | | |
| * **Integrity** | Only authorized personnel can modify this information asset, as follows: | | **Paul Evans,**  **Sally McCarty,**  **Manager Software Development Sam Gold,**  **Supervisor Information Security Alan Brown,**  **Programmer Mick Harris.**  **Employees must be competent at understanding and writing code. Therefore must need to have programing or security skills.** | | |
| * **Availability** | This asset must be available for these personnel to do their jobs, as follows: | | **The product source code must be available whenever someone wants to view or edit it. It must be available to the software activity team for their activities.** | | |
| This asset must be available for 11 hours, 5 days/week, 52 weeks/year. | | The product source code only needs to be available during the work hours of employees who need access to it. As it is specifically the source code and not the actual software sales, customers and other employees do not need to access it. It is presumed the employees who need access work 40 hours a week in a five day working week. However users need time for a breaks and lunch as well as overtime if there is an issue with code on that day. This is why 11 hours has been chosen to account for this. | | |
| * **Other** | This asset has special regulatory compliance protection requirements, as follows: | |  | | |
| **(6) Most Important Security Requirement**  *What is the most important security requirement for this information asset?* | | | | | |
| * Confidentiality | * Integrity | * Availability | | | * Other |

ABC Technologies does not want the source code to be leaked as it is one of the crucial assets (PECB 2011). This is considered a crucial asset as it foundation of what the software activity side of the organisation as it is the only products they provide as a service and sell. This is the only source of known income from the software side of the organisation therefore it must be considered a crucial asset not just because ABC Technologies says it is.

The source code of a product in a software company is considered a high-risk asset because it is essential to the company's operations and requires dedicated attention from a department or team. If the source code is not protected, it could result in significant consequences that may be difficult to repair. Regular reporting on the source code allows for close monitoring and helps ABC Technologies maintain its level of service. It also brings awareness of the risk to higher authorities and aids in the company's business continuity plan. Proper budgeting for the replacement of the source code and monitoring its maintenance helps prioritize resources and identify lower-risk assets that may require attention (SPM Assets, 2022).

The confidentiality of product source code is important for several reasons:

* The source code of a product often contains proprietary information and trade secrets that are critical to the competitive advantage of a software company. If the confidentiality of the source code is compromised, it could lead to the theft of these trade secrets and intellectual property, resulting in financial losses and damage to the company's reputation.
* If the source code falls into the wrong hands, it could be accessed or used without authorisation. This could lead to the creation of unauthorised copies or variations of the product, resulting in lost revenue for the company.
* The source code of a product can contain vulnerabilities or security flaws that, if discovered by malicious actors, could be exploited to gain unauthorised access or control over the product. Ensuring the confidentiality of the source code helps to prevent such vulnerabilities from being exposed and exploited.
* Customers entrust their personal and sensitive information to software products, and the confidentiality of the source code is crucial for maintaining their trust. If the source code is not kept confidential, it could lead to customer dissatisfaction and potentially even legal liabilities for the company.

(Evans & Bement, 2004)

Only those identified above in worksheet 8 should have access to the product source code to ensure confidentiality is maintained. This is the most important security requirement because it ensures that any unauthorised users cannot view or gain any of the product source code the organisation does not want to disclose. ABC Technologies may not want to disclose this because of known vulnerability’s that can be identified once the code is looked at as well as not giving away any trade secrets. This helps ABC Technologies stay competitive in the market as features their software may not have been developed by competitors. To stay competitive in the market it is imperative that the source code is kept confidential.

The integrity of product source code is important for several reasons:

* Ensuring the accuracy and consistency of the product: If the integrity of the source code is compromised, it could result in errors or inconsistencies in the product, leading to customer dissatisfaction and potentially even legal liabilities for the company.
* Maintaining the reliability and trustworthiness of the product: Customers rely on the integrity of software products to perform as intended and to protect their personal and sensitive information. If the integrity of the source code is compromised, it could lead to a loss of trust in the product and the company.
* Protecting against cyber-attacks: Source code with integrity vulnerabilities can be exploited by malicious actors to gain unauthorised access or control over the product. Ensuring the integrity of the source code helps to prevent such attacks and protect the product and its users.
* Ensuring compliance with industry standards: Many industries have strict regulations and standards for software products, and the integrity of the source code is often a key factor in meeting these standards. If the integrity of the source code is compromised, it could lead to non-compliance and potential legal liabilities for the company.

(Taherdoost H et al., (2013).

Only those identified above in worksheet 8 should have access to the product source code to ensure integrity is maintained.

The availability of product source code is important for several reasons:

* If the source code is not available, it can prevent the company from being able to make changes or updates to the product, leading to missed opportunities and potential loss of revenue.
* If the source code is not available, it can prevent the product from functioning properly, leading to customer dissatisfaction and potential loss of revenue.
* If the source code is not available in the event of a system failure, it can prevent the company from being able to restore the product to normal operation, leading to lost revenue and damage to the company's reputation.
* The availability of the source code is often critical for the continuity of business operations, as it enables the company to make necessary changes and updates to the product.

(Yoseviano, H.F. 2018)

The availability of product source code is important for enabling changes and updates to the product, maintaining its functionality, protecting against system failures, and ensuring the continuity of business operations. Only those identified above in worksheet 8 should have access to the product source code and when they need it which is the users working hours to ensure availability is maintained (Yoseviano, H.F. 2018).

|  |  |  |
| --- | --- | --- |
| **Allegro Worksheet 9a** | **Information Asset Risk Environment Map (Technical)** | |
| **Internal** | | |
| **Container Description** | | **Owner(s)** |
| 1. ABC Technologies Internal networks. All of ABC Technologies traffic passes through here like financial and customer data before being transferred to third party databases. | | **Managed by ABC Technologies IT Department.** |
|  |
| 1. Employee workstations – where employees work from inside and outside the office. | | **Managed by ABC Technologies IT Department.** |
|  |
| 1. Product source code is used to create the software that ABC Technologies sells as a service. | | **Software activity Team** |
| **CEO Sabrina Senet** |
|  | |  |
|  |
| **External** | | |
| **Container Description** | | **Owner(s)** |
| 1. Software=as=a=Service environment.   A database run on the clod by a third party with data centers located in UK, USA and India. | | **ABCloud** |
|  |
| 1. Remote access. Employees can use remote access to access the company’s network from devices not in the company’s office locations. | | **Unknown** |
|  |
| 1. SoftProd adatabase which contains information on ABC’s products. In the situation of ABC Technologies SoftProd only provides the service of their database software. | | **Unknown** |
|  |
|  | |  |
|  |

**Internal**

**Internal Networks**

The internal network is typically considered an information asset risk environment because it is a network that is owned and controlled by an organisation. The purpose of the internal network is to store, process, and transmit a variety of sensitive and confidential information. This information can include financial data, personal information about employees and customers, intellectual property, and other types of sensitive data (Alexander, D. et al. 2013). As a result, the internal network is a critical asset for an organisation, and it is important to protect it from unauthorised access or tampering, as well as from threats such as malware, ransomware, and other types of cyber-attacks. This requires careful planning and management to ensure that the internal network is secure and that the information it contains is protected.

**Employee workstations**

Employee workstations are often considered a potential risk to the confidentiality, integrity, and availability of an organisation's sensitive and confidential information because they are frequently used to store, process, and transmit this type of data (Alexander, D. et al. 2013). To protect these assets, it is important for ABC Technologies takes steps to secure employee workstations and prevent unauthorised access or tampering, as well as to protect against cyber threats.

There are several reasons why employee workstations are considered a risk environment:

* They are often used to access sensitive and confidential information, which makes them a target for cyber criminals.
* They may be connected to the internet, which exposes them to a range of external threats.
* They may be used to access and transmit sensitive information over email or other networks, which can increase the risk of data breaches.
* Employees may not always be aware of the importance of protecting their workstations, and may not follow proper security protocols.

**Product source code**

Source code is often classified as a potential risk to an organisation's sensitive and confidential information because it is a critical asset that is frequently stored, processed, and transmitted on internal networks and workstations. As the underlying set of instructions that dictate the behavior and functionality of a software application or system, source code is typically protected as intellectual property and must be safeguarded against unauthorised access or tampering.

**External**

**SoftProd**

SoftProd is a database that contains information on ABC’s products and only provides the service of their database. There is a high amount of trust between both parties as SoftProd is storing ABC Technologies products that they can easily take especially if there are no contracts in place.

**Remote access**

Remote access refers to the ability to access a computer or network from a remote location, typically over the internet. Remote access is often considered an information asset risk environment because it allows individuals to access sensitive and confidential information from anywhere, at any time. This can increase the risk of data breaches and other security incidents if proper safeguards are not in place. It is not possible for ABC Technologies to see what is happening where the user is working like in an office environment. Presuming the employee has a family their family may use the employees laptop without them knowing if the leave it unattended. This is one of the main risks unauthorised users being in the internal network.

There are several reasons why remote access is considered a risk environment:

* It allows individuals to access sensitive and confidential information from anywhere, at any time, which can increase the risk of data breaches.
* It may be accessed over the internet, which exposes it to external threats such as malware, ransomware, and other types of cyber-attacks.
* It may be accessed by multiple individuals or teams within an organization, which can increase the risk of data breaches.
* It may not be adequately secured, which can increase the risk of unauthorized access or tampering.

(Kassa, S.G. and CISA, C. 2017)

**Software as a Service environment**

Software as a Service (SaaS) refers to a model of software delivery in which a software application is hosted by a third-party provider and made available to customers over the internet. SaaS is often considered an information asset risk environment because it allows users to access sensitive and confidential information from anywhere, at any time. This can increase the risk of data breaches and other security incidents if proper safeguards are not in place. This is the case with ABC Technologies as there is not contract in place with what exact security requirements need to be in place between ABC Technologies and ABCloud. This means that ABCloud only need to manage the data in the cloud servers with the bare minimum legal requirements. Another is that since there is no contract in place someone could try to impersonate an ABC Technologies employee to try and obtain sensitive information (Mackie. R, 2016).

There are several reasons why SaaS is considered a risk environment:

* It allows users to access sensitive and confidential information from anywhere, at any time, which can increase the risk of data breaches.
* It may be accessed over the internet, which exposes it to external threats such as malware, ransomware, and other types of cyber attacks.
* It may be accessed by multiple users within an organization, which can increase the risk of data breaches.
* The security of the SaaS application and the provider's infrastructure may not be adequately managed, which can increase the risk of unauthorized access or tampering.

(Mackie. R, 2016)

|  |  |  |
| --- | --- | --- |
| **Allegro Worksheet 9b** | **Information Asset Risk Environment Map (Physical)** | |
| **Internal** | | |
| **Container Description** | | **Owner(s)** |
| 1. Paper copies of source code either written or printed by software activity staff. | | **Software activity staff** |
|  |
| 1. Data stored on computers that are printed or written on paper. | | **Software activity staff** |
|  |
|  | |  |
|  |
|  | |  |
|  |
| **External** | | |
| **Container Description** | | **Owner(s)** |
| 1. Physical access control at the office of ABC Technologies is outsourced by a leasing company. As they manage the office they potentially have access to the office at any time. | | **Leasing company** |
|  |
|  | |  |
|  |
|  | |  |
|  |
|  | |  |
|  |

**Internal**

**Paper copies of source code and other paper copies of data**

The following are reasons why paper copies are issues for security:

**Physical security:** Paper copies of source code are vulnerable to physical threats such as theft, loss, or damage. Once the source code is in paper form, it can be easily stolen, lost or destroyed, potentially falling into the hands of malicious actors who can use it to exploit vulnerabilities in the software or develop malicious software.

**Version control:** Paper copies of source code can make it difficult to manage version control. If multiple versions of the source code are printed, it can be difficult to determine which version is the most current, increasing the risk of using outdated code that may contain known vulnerabilities (Whitman et al., 2020).

**Lack of access control:** Paper copies of source code lack the access controls that are typically used to protect electronic copies of code, such as user authentication, permissions and access controls. This makes it easy for unauthorised users to gain access to the source code, increasing the risk of it being compromised. ABC Technologies there has been an incident with cleaners getting their hands on paper copies of source code and have issues leaving papers on desks over the weekend (PECB 2011).

**Limited collaboration:** Paper copies of source code can make it difficult for software development teams to collaborate effectively, as it can be time-consuming and error-prone to distribute and share paper copies of code among team members.

**Auditing:** If code is only written down or printed and then only changed on the paper, it can be hard to track who made edits to the code and when. This causes issues when making it hard when code reviews and audits need to be done to identify any security issues (Whitman et al., 2020).

**External**

There are a few issues with outsourcing physical security:

* **Loss of control:** When security is outsourced, ABC Technologies may have less control over the security measures that are implemented and how they are administered. This can make it more difficult to ensure that security measures are aligned with the company's needs and goals.
* **Reduced flexibility:** Outsourcing security can limit ABC Technologies ability to adapt and respond to changing security threats and requirements. It may also be more difficult to implement new or custom security measures, as the company is reliant on the service provider to make changes.
* **Increased costs:** Outsourcing security can be more expensive than managing security in-house, particularly if the company has to pay for additional services or support.
* **Reduced transparency:** When security is outsourced, it may be more difficult for ABC Technologies to understand and monitor the security measures that are in place, and to identify and resolve security issues.
* **Dependence on the provider:** ABC Technologies will be dependent on the provider to deliver the promised security service and performance. Any issues with the provider, like a lack of knowledge or unresponsiveness, it will directly affect the security and protection of the company.

These might already be an issue as there is no clear indication of any contractual obligations that have been set by either party for securing the office (PECB 2011).

|  |  |  |
| --- | --- | --- |
| **Allegro Worksheet 9c** | **Information Asset Risk Environment Map (People)** | |
| **Internal Personnel** | | |
| **Name or Role/Responsibility** | | **Department or Unit** |
| 1. IT Team | | **IT department** |
|  |
| 1. Software activity team | | **Software activity department** |
|  |
| 1. Jenifer Gordon | | **Administration team** |
|  |
|  | |  |
|  |
| **External Personnel** | | |
| **Contractor, Vendor, Etc.** | | **Organization** |
| 1. Software-as-a-Service (SaaS) provider. | | **AB Cloud** |
|  |
| 1. Corporate website that was built by a website  development company that takes responsibilities of relevant updates. | | **Unknown** |
|  |
| 1. Access control from remote devices | | **Unknown leasing company** |
|  |
|  | |  |
|  |

**Internal**

**IT Team**

The IT team is crucial for ensuring the security of an organisation, as they are responsible for implementing and maintaining security measures to protect ABC Technologies networks, systems, and data from cyber threats and breaches. This includes tasks like setting up firewalls, installing and updating antivirus software, monitoring network activity for suspicious activity, and conducting regular security audits. Additionally, the IT team is responsible for developing and implementing security policies and procedures, as well as providing training and education for employees on how to identify and prevent security risks. The IT team plays a key role in protecting the organisation from potential cyber-attacks and ensuring the confidentiality, integrity, and availability of all IT services under control of ABC Technologies.

**Software Activity Team**

ABC Technologies software activity team is considered an information asset risk because of the following:

Firstly the software activity team has access to sensitive information such as trade secrets, customer data, and financial information. If this information falls into the wrong hands, it can cause significant harm to the organisation.

The second reason is the software activity team is often distributed and may be working with third-party vendors, which can increase the risk of data breaches and other security incidents.

Finally, a software development team can also be an information asset risk if they don't follow the organisation's security policies and procedures and their activities are not properly monitored. This can lead to security vulnerabilities and other issues that can put the organization at risk.

(PECB, 2011)

**Jenifer Gordon**

Jenifer’s contract was never signed, as she is the payroll supervisor they have a lot of information about the financials of the company. Due to the contract not being signed Jenifer has no contractual obligations to keep any information about ABC Technologies secret. This leads to the issue of confidentiality and because there is no contract in place it means ABC Technologies cannot do anything if Jenifer leaks any information (PECB, 2011).

**External**

**Access control from remote devices**

Remote devices are used at ABC Technologies for employees who work from home and allow an individual access to the organisations network. As the device is not secure in the organisations office it increases the risk of unauthorised access to sensitive information as well as the potential for security breaches and other incidents. Sally McCarty the vice-president lost her laptop, if the remote access system is not properly secured, it can be vulnerable to cyber-attacks, and this can allow hackers to gain access to network and bypass security controls. Another issue is communication between ABC Technologies and the remote access company may be poor leading to a risk where an employee with access to the remote access system leaves the organisation or their access is not revoked; resulting in the ex-employee still having access to the organisation's security systems and sensitive information.

**Corporate website**

There is no suggestion that ABC Technologies has any control over the webpage as there is no evident contract in place in regards to how it is managed and secured (PECB, 2011). This leaves ABC Technologies in the dark with their company name out there the third part company could ruin ABC Technologies reputation by adding comments ABC Technologies do not agree with. The third party is not known so it is unknown if they are reputable. Additionally the minimum security requirements for the webpage are not clear and needs addressing.

**Software-as-a-Service (SaaS) provider.**

The SaaS provider holds any information in which ABC Technologies saves in the cloud servers. There is no agreement in place for minimum security requirements for the database, so is presumed that the minimum amount of security is applied to the cloud server (PECB, 2011). Additionally if the cloud server goes down ABC Technologies will have issues with availability. However it is presumed that AB Cloud has relevant procedures in place to ensure servers are always working.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10a** | | | **Information Asset Risk Worksheet** | | | | | |
| **Information Asset Risk** | **Threat** | Information Asset | Product Source Code | | | | | |
| Area of Concern | *Paper copies of product source code are left on the desks and not securely put away or destroyed before the cleaners come in the evening after work hours.* | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | Cleaning staff | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | Sees product source code while cleaning | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | Curiosity | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | Only authorised personnel can view this information asset. | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High** | * **Medium** | | * **Low** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| Exposure of the source code can lead to the company’s reputation decrease and customer confidence. | | | | Reputation & Customer  Confidence 5 | | Med | 10 |
| Financial 5 | | Low | 5 |
| **ABC Technologies perception of the quality of work could be criticised if leaked source code is not written to high standards.** | | | | Productivity 4 | | Low | 4 |
| Safety & Health 1 | | Low | 1 |
|  | | | | Fines & Legal Penalties 2 | | Low | 2 |
| User Defined Impact Area | |  |  |
| **Relative Risk Score** | | | | | | | | **22** |

|  |  |
| --- | --- |
| **Relative Risk Score** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Software Activity staff | * To ensure paper information is being handled correctly regular audits can be performed. * Ensure all paper copies that are no longer needed are correctly destroyed (shredded) when no longer needed by the company. * Provide regular training about the importance of ensuring confidentiality and integrity in the workplace. * Introduce a policy where all paper copies of any asset are locked in filing cabinets when not being used. * Introduce a non-disclosure policy that all software activity staff must sign with the agreement of ABC Technologies.   (ISO, 2013) | | | |
| Cleaning staff | * Introduce a non-disclosure policy that all cleaning staff must sign with the agreement of ABC Technologies.   (ISO, 2013) | | | |
|  |  | | | |
|  |  | | | |
|  |  | | | |
|  |  | | | |

ABC Technologies values the confidentiality and protection of its trade secrets and intellectual property represented by the source code. By implementing controls above, it ensures that this valuable asset is kept confidential and not disclosed or stolen. Nonetheless, it is essential to acknowledge that source code is not impervious and may contain vulnerabilities. Therefore, these controls serve to prevent exploitation by malicious actors while maintaining its security. Additionally, it guarantees ABC Technologies compliance with laws and regulations (Wolford, B., 2021) and helps to preserve the company's reputation and trust with customers.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
|  | **Threat** | Information Asset | Product source code | | | | | |
| Area of Concern | *Cyber attack on the product source code* | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | A black hat attacker stealing product source code to sell to a competitor. | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | The hacker gains accesses to the network between the developer and cloud server. | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | Financial gain | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | The confidentiality of the product source code will be breached and other data being sent between the networks. | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High** | * **Medium** | | * **Low** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| Financial loss from: paying the attacker for not leaking code and loss of trade secret. | | | | Reputation & Customer  Confidence 4 | | High | 12 |
| Financial 5 | | High | 15 |
| There will be a loss in customer confidence and reputation in the market for ABC Technologies code the hacker stole is reported by external parties. E.g. the news. | | | | Productivity 3 | | Medium | 6 |
| Safety & Health 2 | | Low | 2 |
| New code would need to be developed to ensure that the leaked code isn’t exploited by malicious users. E.g. reverse engineering the code to find sensitive data from the live environment. | | | | Fines & Legal Penalties 1 | | Low | 1 |
| User Defined Impact Area | | 0 | 0 |
| **Relative Risk Score** | | | | | | | | **36** |

|  |  |
| --- | --- |
| **Relative Risk Score** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Management | * Implementing policies and procedures for managing access to the source code, including guidelines for creating and managing user accounts, setting and enforcing strong passwords, and regularly reviewing and revoking access as needed * Conducting background checks on employees who will have access to the source code * Training employees on cyber security best practices, including how to identify and report potential cyber threats * Ensuring that all employees who have access to the source code are aware of their responsibilities in protecting it   SANS Institute (n.d.), (NIST n.d.). | | | |
| IT Supervisor | * Implementing network security measures, such as firewalls and intrusion detection systems, to prevent unauthorised access to the source code * Implementing authentication and authorisation controls to ensure that only authorised users have access to the source code * Encrypting the source code while it is in transit and at rest to prevent unauthorised access * Regularly updating and patching the software and systems used to manage and store the source code   SANS Institute (n.d.), (NIST n.d.). | | | |
| Network Technicians | * Storing the source code in a secure location, such as a locked room or cabinet, to prevent unauthorised access * Limiting access to the source code to authorised personnel only * Implementing security measures to prevent unauthorised physical access to the location where the source code is stored, such as security guards, cameras, and access control systems   SANS Institute (n.d.), (NIST n.d.). | | | |
|  |  | | | |

Even with the implementation of these controls, there may still be some residual risk that is accepted by the organisation. This risk could include the possibility of a cyber-attack or other security incident occurring despite the implementation of controls, or the risk of damage or loss to the source code due to natural disasters or other events beyond the control of the organisation. It is important for organisation to carefully assess the risks they are willing to accept and to implement controls that are appropriate for their specific situation (CISA) n.d).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
|  | **Threat** | Information Asset | Source code | | | | | |
| Area of Concern | *Unintentional change in product source code causing issues with the product software.* | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | Programmer Mick Harris. | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | Accidently updated the live environment when testing the new patch. | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | There was no motive and was an accident. | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | The availability of software would have been compromised. | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High** | * **Medium** | | * **Low** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| Financial loss for the company. | | | | Reputation & Customer  Confidence 3 | | Medium | 6 |
| Financial 4 | | Medium | 8 |
| Delay for the next version of the software caused by unavailability of the software. | | | | Productivity 5 | | Medium | 10 |
| Safety & Health 1 | | Low | 1 |
|  | | | | Fines & Legal Penalties 3 | | Low | 3 |
| User Defined Impact Area | |  |  |
| **Relative Risk Score** | | | | | | | | **28** |

|  |  |
| --- | --- |
| **Relative Risk Score** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Administrative controls | * Implement a formal change management process that requires all changes to the source code to be reviewed and approved by a designated team or individual before being implemented. * Establish clear roles and responsibilities for managing and maintaining the source code. * Implement a system for tracking and documenting all changes made to the source code.   Nicolette, D. (n.d). | | | |
| Technical controls | * Use version control software, such as Git, to manage and track changes to the source code. * Implement automated testing and continuous integration processes to catch any issues that may be introduced with code changes. * Use static code analysis tools to identify potential issues with the code before it is implemented.   International Monetary Fund (n.d). | | | |
| Physical controls | * Store the source code in a secure location, such as a secure server or cloud-based repository that is accessible only to authorised personnel. * Implement access controls to prevent unauthorised individuals from accessing the source code.   Nicolette, D. (n.d). | | | |
|  |  | | | |

Even with these controls in place, there may still be some residual risk that is accepted by the organization. For example, if an authorized individual makes an unintentional mistake while making a change to the source code, it could still cause issues with the product software. The organisation may need to have processes in place to quickly identify and resolve any issues that do arise in order to minimise the impact on the product and the organisation (Project Management Institute n.d).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat Scenario Questionnaire 1** | **Technical Containers** | | | |
| **This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is “yes” consider whether the scenario could occur accidentally or intentionally or both.** | | | | |
| **Scenario 1:** Think about the people who work in your organization. Is there a situation in which an employee could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be: | | | | |
| Disclosed to unauthorized individuals? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Modified so that it is not usable for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Interrupted so that it cannot be accessed for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Permanently destroyed or temporarily lost so that it cannot be used for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| **Scenario 2:** Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be: | | | | |
| Disclosed to unauthorized individuals? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Modified so that it is not usable for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Interrupted so that it cannot be accessed for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Permanently destroyed or temporarily lost so that it cannot be used for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Threat Scenario Questionnaire – 1 (cont)** | | | **Technical Containers** | | | |
| **Scenario 3:**  In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:   * Unintended disclosure of your information asset * Unintended modification of your information asset * Unintended interruption of the availability of your information asset * Unintended permanent destruction or temporary loss of your information asset | | | | | | |
| A software defect occurs | **No** | **Yes (disclosure)** | | **Yes (modification)** | **Yes (interruption)** | **Yes (loss)** |
| A system crash of known or unknown origin occurs | **No** | **Yes (disclosure)** | | **Yes (modification)** | **Ye  (interruption)** | **Yes (loss)** |
| A hardware defect occurs | **No** | **Yes (disclosure)** | | **Yes (modification)** | **Yes (interruption)** | **Yes (loss)** |
| Malicious code (such as a virus, worm, Trojan horse, or back door) is executed | **No** | **Yes (disclosure)** | | **Yes (modification)** | **Yes (interruption)** | **Yes (loss)** |
| Power supply to technical containers is interrupted | **No** | **Yes (disclosure)** | | **Yes (modification)** | **Yes (interruption)** | **Yes (loss)** |
| Problems with telecommunications occur | **No** | **Yes (disclosure)** | | **Yes (modification)** | **Yes (interruption)** | **Yes (loss)** |
| Other third-party problems or systems | **No** | **Yes (disclosure)** | | **Yes (modification)** | **Yes (interruption)** | **Yes (loss)** |
| Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur | **No** | **Yes (disclosure)** | | **Yes (modification)** | **Yes (interruption)** | **Yes (loss)** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat Scenario Questionnaire – 2** | **Physical Containers** | | | |
| **This worksheet will help you to think about scenarios that could affect your information asset on the physical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is “yes” consider whether the scenario could occur accidentally or intentionally or both.** | | | | |
| **Scenario 1:**  Think about the people who work in your organization. Is there a situation in which an employee could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be: | | | | |
| Disclosed to unauthorized individuals? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Modified so that it is not usable for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Interrupted so that it cannot be accessed for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Permanently destroyed or temporarily lost so that it cannot be used for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| **Scenario 2:**  Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be: | | | | |
| Disclosed to unauthorized individuals? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Modified so that it is not usable for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Interrupted so that it cannot be accessed for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Permanently destroyed or temporarily lost so that it cannot be used for intended purposes? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Threat Scenario Questionnaire -2 (cont)** | | | **Physical Containers** | | | |
| **Scenario 3:**  In this scenario, consider situations that could affect your physical containers and, by default, affect your information asset. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:   * Unintended disclosure of your information asset * Unintended modification of your information asset * Unintended interruption of the availability of your information asset * Unintended permanent destruction or temporary loss of your information asset | | | | | | |
| Other third-party problems occur | **No** | **Yes  (disclosure)** | | **Yes  (modification)** | **Yes  (interruption)** | **Yes (loss)** |
| Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur | **No** | **Yes  (disclosure)** | | **Yes  (modification)** | **Yes  (interruption)** | **Yes (loss)** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat Scenario Questionnaire – 3** | **People** | | | |
| **This worksheet will help you to think about scenarios that could affect your information asset because it is known by key personnel in the organization. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is “yes” consider whether the scenario could occur accidentally or intentionally or both.** | | | | |
| **Scenario 1:**  Think about the people who work in your organization. Is there a situation in which an employee has detailed knowledge of your information asset and could, *accidentally* or *intentionally*, cause the information asset to be: | | | | |
| Disclosed to unauthorized individuals? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Modified so that it is not usable for intended purposes?[[1]](#footnote-1) | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Interrupted so that it cannot be accessed for intended purposes?[[2]](#footnote-2) | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?[[3]](#footnote-3) | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |
| **Scenario 2:**  Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could, *accidentally* or *intentionally*, cause your information asset to be: | | | | |
| Disclosed to unauthorized individuals? | | **No** | **Yes  (accidentally)** | **Yes  (intentionally)** |

**Bibliography Worksheets 1-7:**

App Direct (2018) *How long does it take to move to the cloud?*, *AppDirect*. Available at: https://www.appdirect.com/blog/how-long-does-it-take-to-move-to-the-cloud (Accessed: December 28, 2022).

Armony, M., Shimkin, N. and Whitt, W. (2009). The Impact of Delay Announcements in Many-Server Queues with Abandonment. Operations Research. [Accessed 30th November 2022]

Ashton. L,(2020), *Data Breach* Compensa*tion Amounts, Data breach help,* <<https://www.data-breaches.co.uk/data-breach-protection-claims-and-compensation/amounts/>>, [Accessed 28th November 2022]

Caralli, R.A., Stevens, J.F., Young, L.R. and Wilson, W.R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.

Calculating Personal Injury claim, < <https://www.accidentclaimsadvice.org.uk/calculating-a-personal-injury-claim/>> [Accessed 28th November 2022]

Calder, A. and Watkins, S. (2010) Information security risk management for ISO27001/ISO27002. Cambridgeshire: IT Governance Pub.

Callaghan, D. and O'Sullivan, C. (2005) “Who should bear the cost of software bugs?,” *Computer Law & Security Review*, 21(1), pp. 56–60. Available at: <https://doi.org/10.1016/j.clsr.2005.01.015>.

Cohen, G. (2021) *Downtime, outages and failures - understanding their true costs*, *Gad Cohen*. Available at: https://www.evolven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html (Accessed: January 6, 2023).

Commission, L.P. (2022) *The National Minimum Wage in 2022*, *GOV.UK*. GOV.UK. Available at: https://www.gov.uk/government/publications/the-national-minimum-wage-in-2022 (Accessed: January 10, 2023).

Crook, Z. (2018) *Outdated technology costs businesses more than it saves*, *Bizjournals.com*. Available at: https://www.bizjournals.com/phoenix/news/2018/11/15/outdated-technology-costs-businesses-more-than-it.html (Accessed: January 7, 2023).

Deskera Content Team, (no date), *What are operating costs?* <<https://www.deskera.com/blog/operating-costs/#what-are-variable-operating-costs>> [Accessed 21th November 2022]

Daswani, N. and Elbayadi, M. (2021) Big breaches: Cybersecurity lessons for everyone. New York, NY: Apress.

Gorecki, A 2020, Cyber Breach Response That Actually Works : Organizational Approach to Managing Residual Risk, John Wiley & Sons, Incorporated, Newark. Available from: ProQuest Ebook Central. [7 January 2023].

HADA, T., OLTEANU, E. and DOBRA, I.B., 2015. ANALYSIS OF THE AVERAGE SHARE PRICE OF COMPANIES LISTED ON BSE DEPENDING ON THE PROFIT AND EXCHANGE SEGMENT. DIFFERENT TECHNIQUES OF GENERAL LEAST SQUARE AND COMPUTING COEFFICIENT COVARIANCE FOR MEAN PRICE EQUATION ESTIMATION.

Health and Safety Executive (2019). Fire safety. [online] Hse.gov.uk. Available at: <https://www.hse.gov.uk/toolbox/fire.htm> (Accessed: January 7, 2023).

Health and Safety Executive (2019a) Slips and trips, Slips and trips - health and safety topics in cleaning. Available at: <https://www.hse.gov.uk/cleaning/topics/slips.htm> (Accessed: January 7, 2023).

Indeed, Editorial Team,(2021), *10 Examples of Operating Costs in Running a Business,* < <https://www.indeed.com/career-advice/career-development/examples-of-operating-costs>> [Accessed 22th November 2022]

Keehler, J. (2022) *Council post: 8 common reasons why marketing campaigns fail*, *Forbes*. Forbes Magazine. Available at: https://www.forbes.com/sites/forbesagencycouncil/2021/08/26/8-common-reasons-why-marketing-campaigns-fail/?sh=6e13a915273d (Accessed: January 6, 2023).

Lawrence, A. (2022) *Is concern over cloud and third-party outages increasing?* [Preprint]. Available at: https://doi.org/https://journal.uptimeinstitute.com/is-concern-over-cloud-and-third-party-outages-increasing/.

Mahalingam, A., Coburn, A., Jung, C. J., Yeo, J. Z., Cooper. G., Evan, T. (2018). Impacts of Severe Natural Catastrophes on Financial Markets.

Marchese. T,(No date), *Top 5 most common workplace injuries and how to avoid them, Workers Comp*, <<https://www.marchesecomp.com/workers-comp/top-5-most-common-workplace-injuries-and-how-to-avoid-them/>> [Accessed 28th November 2022]

Professional Evaluation and Certification Board [PECB], 2011. Case Study ABC Technologies. [Online] Professional Evaluation and Certification Board, p1-12. Available at:<https://bradford.instructure.com/courses/18231/modules/items/353753>.

Rosenthal. M (2022), *Insider Threats Examples: 17 Real Examples of Insider Threats*, <<https://www.tessian.com/blog/insider-threats-types-and-real-world-examples/>> [Accessed 25th November 2022]

Suroso, J.S. and Fakhrozi, M.A. (2018). Assessment of Information System Risk Management with Octave Allegro at Education Institution. Procedia Computer Science.

Sutton, D. and Taylor, A. (2013). Information security management principles. Bcs Learning & Development Lim. [Accessed 29th November 2022]

Tasya, M.A., Suwawi, D.D.J. and Utomo, R.G. (2022). Information Security Risk Analysis of State-Owned Bank Information Technology (IT) Assets Using the Octave Allegro Method. J-SAKTI (Jurnal Sains Komputer dan Informatika). [Accessed 30th November 2022]

Tellis, G.J. (2003) *Effective advertising: Understanding when, how, and why advertising works*. Thousand Oaks, Calif: Sage Publ.

UK GOV. (2015) Fire safety in the Workplace, GOV.UK. GOV.UK. Available at: https://www.gov.uk/workplace-fire-safety-your-responsibilities/enforcement-appeals-and-penalties (Accessed: December 19, 2022).

UK GOV (2022). OFSI enforcement and monetary penalties for breaches of financial sanctions Guidance. [online] Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083299/15.06.22_OFSI_enforcement_guidance.pdf>.

Whitman, M.E. and Mattord, H.J. (2018). Principles of information security. 6th ed. Boston, Mass.: Cengage Learning. [Accessed 30th November 2022]

Yurday, E. (2023) Average cost of electricity per kwh in the UK 2023, NimbleFins. NimbleFins. Available at: https://www.nimblefins.co.uk/average-cost-electricity-kwh-uk (Accessed: January 10, 2023).

Zhang, Q., Wang, J., Lu, A., Wang, S. and Ma, J. (2018). An improved SMO algorithm for financial credit risk assessment – Evidence from China’s banking. [Accessed 30th November 2022]

Zhu, H. (2020) Online meta-learning firewall to prevent phishing attacks - neural computing and applications, SpringerLink. Springer London. Available at: https://link.springer.com/article/10.1007/s00521-020-05041-z (Accessed: January 10, 2023).

**Bibliography Worksheets 8-10:**

Alexander, D. et al. (2013) Information security management principles. Swindon: BCS, The Chartered Institute for IT.

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). Cybersecurity for Small Businesses. Retrieved from <https://www.cisa.gov/cybersecurity-small-businesses>

Evans, D. and Bement, P. (2004) *Standards for security categorization of Federal Information and Information Systems*. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. Geneva, Switzerland.

International Monetary Fund. (n.d.). "Risk Management: Basic Concepts". Retrieved from <https://www.imf.org/en/Publications/FM/issues/2019/12/31/risk-management-basic-concepts-46147>

Kassa, S.G. and CISA, C. (2017). IT asset valuation, risk assessment and control implementation model, Available at: [https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation .model#:~:text=Mapping%20an%20information%20asset%20(such,transporting%20and%20processing%20the%20asset.](https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation%20.model#:~:text=Mapping%20an%20information%20asset%20(such,transporting%20and%20processing%20the%20asset.) Accessed Via Internet: 16/12/2022

National Institute of Standards and Technology (NIST). (n.d.). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from <https://www.nist.gov/cybersecurity/protecting-controlled-unclassified-information-nonfederal-systems-and-organizations>

Nicolette, D. (n.d.). "Source Code Management Best Practices". Retrieved from <https://www.perforce.com/blog/qac/source-code-management-best-practices>

Mackie. R, (2016), To Include or Not to Include – Scoping ISO 27001 and Colocation Service Providers, Accessed via Internet 09/12/2022, < <https://www.schellman.com/blog/to-include-or-not-to-include-scoping-iso-27001-and-colocation-service-providers>>

Professional Evaluation and Certification Board (PECB), (2011). Case Study ABC Technologies. [Online]   
Professional Evaluation and Certification Board, p1-12. Available at:   
https://bradford.instructure.com/courses/18231/modules/items/353753

Project Management Institute. (n.d.). "Best Practices for Change Management". Retrieved from <https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/best-practices-for-change-management.pdf>

SANS Institute. (n.d.). Protecting Source Code. Retrieved from <https://www.sans.org/security-resources/policies/general/pdf/protecting-source-code>

SPM Assets (2022) Why understanding critical assets is so important, Why Understanding Critical Assets is so Important. SPM Assets. Available at: https://www.spmassets.com/news/why-you-should-frequently-report-on-your-most-critical-assets#:~:text=Prioritising%20resources%3A%20Identification%20and%20awareness,receive%20disproportionate%20attention%20and%20expenditure (Accessed: January 2, 2023).

Taherdoost, H., Chaeikar, S. S., Jafari, M., & Shojae Chaei Kar, N. (2013). Definitions and Criteria of CIA Security Triangle in Electronic Voting System. International Journal of Advanced Computer Science and Information Technology (IJACSIT) Vol, 1, 14-24.

Whitman, M.E., Mattord, H.J. and Gim, T. (2020) *Jeongbo Boho wolli*. Seoul: Hongneung.

Wolford, B., (2021). What is GDPR, the EU's new data protection law? - **GDPR.eu**. [online] GDPR.eu. Available at: <https://gdpr.eu/what-is-gdpr/> [Accessed 7 July 2021]

Yoseviano, H.F. (2018) *The use of ISO/IEC 27001: 2009 to analyze the risk and ... - IEEE xplore*. Available at: https://ieeexplore.ieee.org/abstract/document/8528096/ (Accessed: January 10, 2023).

1. [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)