***Project Overview***

*This project is intended to have you start thinking about and planning your own cybersecurity program. When possible, use actual data and information from your own organization. You might already be aware of this data or can get it through interviews with key people in your own organization or vendors.*

1. **Current Threats**

Research **one** of the top critical cyber threats and risks facing your current organization or your industry. For the threat you identified, respond to the following 5 prompts:

*( Your response for each item below should include at least 1 sentence)*

|  |
| --- |
| 1. Identify the type of threat you selected. **Bringing data in the Public Cloud and have the risk of Randsomware or data Breach** |
| 1. Explain how the threat is (either) external or internal.  **This is an external thread where probably Phishing is needed to get to the Data. So partly internal as well.** |
| 1. Explain how the threat is (either) real or perceived.   The Thread is real since every one working with Data and storing it in the cloud can become a victom of Phishing |
| 1. Explain how the threat is detected?  Unusual emails being sent, exeptional Amounts of Data Movements detected |
| 1. Explain how the threat is a (pick one) low, med, or high.   High Risk – you never know which data is being effected. What Company Secrets or Customer Information is being Revealed. |
| 1. Briefly describe any recent breach from this threat   Github got Breached – Probably by a Phising email to a Developer |

1. **Enterprise Risk Management**

Begin to create an ERM plan based on your organization's *most valued products or services by* completing the sections below.

* Identify all executives and managers in your organization who should share responsibility for ERM. Please include the job title only. Your list should include at least 5 positions.

|  |
| --- |
| * CIO * CFO * CISO * CEO |

* What is your organization’s current **risk appetite**? What is the management's **willingness to risk**? Please provide 1 sentence response for each item below.

|  |
| --- |
| What are the long-term cybersecurity objectives for your organization?   * Risk Appetit is Low – and very districtive – only encrypted data may land in the cloud |
| Describe what stage(Planning, Growth, Maturity, Decline) your organization is currently experiencing.   * Planning how to ensure secure Cloud Platform Operations |
| Describe the current financial status/stability of your organization   * Stabil |
| Describe your organization’s risk capacity   * The Organisation has a Cyber Group – But Cyber Security Awareness needs to grow inside the company |

* Choose any single business unit from your organization and respond to the questions below.

|  |
| --- |
| Business unit name: Platform Engineering  1. What are the biggest threats to this department? (identify at least 3)   * Introducing Vulnerable Software into cloud for Data Processing * Hijacking of KEYStore * Tokens being open – Secrets not stored in a Keystore but Hard-coded |
| 2. Select any 1 of the threats identified above. Using the document provided or the link below for a **5X5 Impact and Probabilty matrix**, complete a risk impact assessment and risk score based on your organizations risk profile. In 1-2 sentences, explain the significance of that threat & risk score for your organization.  Selected threat: Hijacking the Keystore  Risk Score: 8  Significance: Disruptive  If the Keystore gets Hijacked they do not yet have the Keys inside it. Since they are encrypted, but still it is an discuption in a sense that Decryption cannot be done for existing objects in the cloud.  Helpful link[: https://laconteconsulting.com/2018/12/02/calculate-impact-and-probability](https://laconteconsulting.com/2018/12/02/calculate-impact-and-probability)/ |

* 3rd Party Vendors
  + - Describe any 2 major vendors used by your organization

|  |
| --- |
| Vendor 1 ACME Secure |
| Vendor 2 CyberCloudicon |

* + - Select one of the above vendors and respond to the following 2 prompts

|  |
| --- |
| Vendor name: Acme Secure |
| 1 Contact the appropriate person to provide the following information.  How do you currently evaluate the cybersecurity posture of the selected vendor? Your response should include at least 2 ways you will proactively evaluate a security posture   * We will have an Security assessment * Pentesting the Application |
| 2 Based on the evaluation that you identified steps above, identify at least 1 recommendation to enhance compliance.   * Using certified Certificates in the Application |

1. **Incident Response (IR) Plan**

Using the following list of incident response activities, identify steps under each that should be taken by your organization

|  |
| --- |
| 1 Preparation (identify at least 2 steps)   * Incident Reporting Mechanism * Contact information for Support – having a list ready |
| 2 Identification (identify at least 3 steps)   * Web server log entries that show the usage of a vulnerability scanner * A host records an auditing configuration change in its log * A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server |
| 3 Containment (identify at least 3 steps)   * Shutdown the system * Change all Passwords * Change IPaddressess |
| 4 Eradication (identify at least 3 steps)   * Deleting Malware * Changing Password from Accounts * Mitigate all vulnarabilities |
| 5 Recovery (identify at least 3 steps)   * Systems will be restored * Remediate Vulnerabilities * Tightening Network perimeter security |
| 6 Lessons Learned (identify at least 3 steps)   * What information was needed sooner – Suspisious Emails * What tools should be in place to detect issues sooner * What precursors should be watched in future? |

1. **Cybersecurity Investments**

Coordinate with your CIO to obtain the following information. Complete the provided 3-year cybersecurity budget table by entering the appropriate financial data for each year. Provide a sentence to justify the financial allocation for each program or technology.

Be sure to address

* + Programs
    - Training ( 3rd party awareness training conducted at least annually and Certifications i.e. Security +, Network+, CISM, CISSP, AWS, ect )
    - Pentesting ( to be conducted at least annually or when/if a breach occurs)
  + Technology or other professional services
    - Hardware ( switches, routers, printers, computers, servers, ect)
    - Software ( licensing agreements, 24/7 maintenance support)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Current year | Second year | Third year |
| Training | 80K | 40K | 30K |
| Pentesting/Professional services | 100K | 100K | 100K |
| Hardware | 500K | 250K | 250K |
| Cyber insurance | 1000K | 1000K | 1000K |
| Software | 500K | 300K | 300K |

Justify your funding decisions for current and future years. Your response should include at least 3 sentences and should reference each topic *(Training, Pentesting/Professional services, Hardware, Software, Cyber insurance)*

|  |
| --- |
| Insuring the Company assets is super important so the highest value goes there. Then at start more Budget is needed for training and getting personell Certified  Then Year after Year Certificates need to be renewed which costs less then a complete training.  On hardware firewals and routers need to be in place and kept up to date.  Thread Detection Software is needed to detect intrusions, the first year will be more expensive as first buy. The following years will be and exention / prolongation of the license therefore costs less. |

1. **Culture Awareness Plan**

Describe the details of an organizational-wide cybersecurity awareness campaign that includes: Phishing, Password, and Remote policy

*( Your response for each item below should include at least 5 specific strategies your company will use to enhance cybersecurity awareness)*

|  |
| --- |
| Phishing/Whaling   * Suspected Emails should be captured and put in Quarantine by the antivirus software on the mailserver * Suspicious internet addresses should be blocked, when clicking a link the link will not work * Having an easy to use SPAM reporting function in place in the company * Doing awareness session for personell about how pishing works and what to watch out for * On the Intranet have an OnePager to make people aware about Phishing. That it is not only email, but also sms and Phone Calls |
| Passwords   * Passwords should be long enough and mixed characters * Passwords should not inlcude reallife words * Passwords should not be reused after a certain period. (Always new passwords) * Passwords need to change every 3 months * Never use the same password on all platforms |
| Remote policy   * When working from a public place, people should have a privacy sreen on their laptop * Devices should have up-to-date Anti-Virus software and frequent scanning * Every device should be secured with a strong password and needs to be locked when leaving it alone, even for the shortest time. * For BYOD policy – Software to control access to company data should be installed so that the company can control the correct use of it. * The opion to install new software on company devices should be controlled by the company. So that only secure and licensed software is being used. |