***Project - Cyber Challenges We Face Today***

***Author: Huy Luu***

*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: **Planning for Cyber Challenges** |
| 1. Explain how the threat is (either) external or internal.   This threat is obviously our internal problems as the cyber challenges is found in company scope and have some impacts for the company and staff. |
| 1. Explain how the threat is (either) real or perceived.   This threat is obviously real problem that all manager and staff must be aware carefully. |
| 1. Explain how the threat is detected?   Via the problems issues that happened on production environment where clients use our products and finally clients raise these problems with leaking security stuff to developer teams so we get this. |
| 1. Explain how the threat is a (pick one) low, med, or high.   The threat is quite high and it really need to be fixed asap and prevent the similar cases in the future. |
| 1. Briefly describe any recent breach from this threat   This security problems has harmful impacts that it results in leaking sensitive personal data of our clients like phone numbers, bank code, and other info. As consequences, clients suffered from attacks from strangers and get the noise from them. |

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.

|  |
| --- |
| * Product owner – prepare for plan * Scrum master – control progress of fixing security problem * Developer – directly fix security problem * Quality assurance – check final result * QC – note all the cases and solutions in official documents |

* 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?   * Limit the alerts, warnings from the system from 1000 to 200 every months |
| Describe what stage(Planning, Growth, Maturity, Decline) your organization is currently experiencing.   * Prepare for specific plan with the name “Problem Limitation” * Get professional to create a plan and specific person to fix alerts, security problems everyday in a week * Note the causes and solutions for every cases they get * Report to leader everyday * Make preparation for any cases happen |
| Describe the current financial status/stability of your organization   * The current financial status of the team is really good with enough budget to implement the cybersecurity plan with 10 million dollars * It is predicted to keep the plan working well in next 3 years * There are still big entrepreneurs willing to sponsor the plan with big budget |
| Describe your organization’s risk capacity   * Risk about the price of the services we use in this plan as its price will increase sharply per months so we worry about the cost in this case. * Example: AWS services will increase at least 10% per 3 months |

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

|  |
| --- |
| Business unit name: Security Preventation Planning  1. What are the biggest threats to this department? (identify at least 3)   * Lack of skilled person * Lack of budget * Shortage of time for fixing as different time among places |
| 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: Security leaking sensitive info of clients  Risk Score: 8/10  Significance: High  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 : **Sonic Cloud company is specialized in cloud solutions for plants for better profits gained.** |
| Vendor 2 : **Jerry technology company is specialized in providing technology infrastructure for small and medium company to gain more clients using their services.** |

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

|  |
| --- |
| Vendor name: **Sonic Cloud company** |
| 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   * Contact our Product manager - Jackson * Contact via mail to developer team lead - Steven |
| 2 Based on the evaluation that you identified steps above, identify at least 1 recommendation to enhance compliance.   * Pay attention to impacting of the security problems and make solutions for preventing them. |

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)   * Get the detailed plan for prevent security problems * Use the modern tools to fix these problems |
| 2 Identification (identify at least 3 steps)   * Get notifications from channels like teams, slack * Via tool for checking cyber security like new relic, pager duty * Check via email, phone |
| 3 Containment (identify at least 3 steps)   * Get the request for contain from clients * Developer use tools to fix this * Note the cases and solutions used in document to reuse later |
| 4 Eradication (identify at least 3 steps)   * Detect type of security problem * Detect impacting level of security problem * Prepare solution and fixing |
| 5 Recovery (identify at least 3 steps)   * Detect the recovery plan * Create the recovery plan * Conduct the plan |
| 6 Lessons Learned (identify at least 3 steps)   * Limit person errors as much as possible * Invest more in technology helps with modern software and tools * Focusing more plan for security issues |

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 | Basic security awareness | Medium security awareness | High security awareness |
| Pentesting/Professional services | Basic tools | Medium tools | High-level tools |
| Hardware | 3x hardware | 5x hardware | 6x hardware |
| Cyber insurance |  |  |  |
| Software | Cyber fish 1 | Cyber Solution | Security problem checker |

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)*

|  |
| --- |
| Conduct basic security awareness in current year and increase the level of all above metrics over the years. |

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   * Phishing/Whaling basic * Phishing/Whaling higher basic * Phishing/Whaling pre-medium * Phishing/Whaling medium * Phishing/Whaling advanced |
| Passwords   * Level 1 password * Level 2 password * Level 3 password * Level 4 password * Level 5 password |
| Remote policy   * Policy for lack of budget * Policy for lack of person * Policy for lack of tool * Policy for lack of time * Policy for lack of plan & solution |