Implementing a Cybersecurity Program

Introduction

Introduction and Scenario	Scenario - Lemonade - Cybersecurity Program You've been hired to come in as a security analyst on a team working for Lemonade. Lemonade, an online insurance company that covers everything from pets to laptops to your home, has been in the process of having an external team work on a cybersecurity program for them to implement. Being a small company, there was no program in place up until now. Lemonade is seeking out a comprehensive program that makes sense for their size and service offerings, most especially as they launched their AI model to predict catastrophes and claims, and uses that data to price their policies. You will be working closely with Nell Crain, CTO to complete this project.	
Requirements Gathering	Requirements gathering is an essential process when setting up a cybersecurity program as it ensures that all stakeholders' expectations are considered, and the program addresses the specific security needs of an organization. It involves identifying and analyzing business objectives, potential risks, regulatory and compliance requirements, and the existing infrastructure to develop a comprehensive security plan. Effective requirements gathering ensures that the cybersecurity program is aligned with the organization's goals, adequately protects against potential threats, and meets compliance standards, ultimately enhancing the organization's overall security posture. It also helps to avoid costly mistakes and ensures that all security solutions are integrated correctly.	

Task	You will have a mock scenario of your first deep-dive discussion with Nell Crain, CTO, who you have now been employed to report to. Your goal will be to identify current concerns, potential requirements, or other risks needing to be addressed by your new cybersecurity program. You will do the following prior to this session: Brainstorm as many questions as come to mind, aiming for at least 15-20 questions. Next, rank the questions assigning the number 1 to the most important question, and so on. Next, refine your questions until you have 7-10 essential questions to drive the interview. Finally, make sure your questions are audience appropriate (non-technical or low-technical) for a CTO to answer Keep in mind that Lemonade has no current cybersecurity program in place, and therefore might not have much information about current state affairs beyond needs and concerns. You Will Know You are Done When **You will know you are done when you have 7-10 high quality questions ready to use in your interviews.**	Conducting Stakeholder Interviews [https://www.clicked.com/learning-experience-page/conducting-stakeholder-interviews-as-a-security-analyst-12-06-23] How to Conduct User Interviews [https://uxdesign.cc/how-to-conduct-user-interviews-fe4b8c34b0b7]
Risk Identification	Identifying risks is crucial when implementing a new cybersecurity program because it helps organizations understand the potential threats and vulnerabilities they may face. It enables them to prioritize resources and allocate budgets accordingly, thereby mitigating the potential impact of a cyber attack. Understanding risks also enables organizations to proactively implement measures to prevent breaches or respond effectively when they do occur.	
Task	In this task, you will leverage the given template (or another tool/method of your preference) to help guide you along your requirements to aid in the identification of a series of risks. You will do the following: Identify 7-10 risks based on your discussion with Nell Crain Research potential additional risks Lemonade as a company may have based on external factors Fill in the information for your template and present your findings to the group You Will Know You are Done When	Focusing on GRC as a Security Analyst Shadow Session: Watch your Coach Momna implement governance, risk, and compliance into their mindset as a GRC Analyst [https://www.clicked.com/learning-experience-page/focusing-on-grc-as-a-security-analyst-2-21-24] Template for your risk

	You have successfully identified and documented a comprehensive list of 7-10 risks stemming from your discussions with Nell Crain and additional research. This list must be aligned with the company's unique circumstances and potential external threats. Your findings are coherently presented, and you are prepared to share and discuss these insights with the group, supporting a more proactive and informed cybersecurity approach.	assessment: IC-Basic-Risk-Assessment-10878.xlsx [https://docs.google.com/spreadsheets/d/1NTVD5Z78cjIgzNwh9sp9E590LckVT3ok/edit#gid=1097821869] Risk Prioritization Shadow Session: Watch Coach Seyi work through different types of risks and how to best prioritize them. [https://www.clicked.com/learning-experience-page/risk-prioritization-strategy-10-18-23] Risk Prioritization Skills Challenge: Watch your peers and coach walk through how to prioritize risk! [https://www.clicked.com/learning-experience-page/risk-prioritization-strategy-10-25-23]
Security Plan Proposals	You will take your requirements information you've compiled and use it to help you create a cybersecurity program proposal to share with your internal team before presenting to Nell Crain. This will require you to use a comprehensive approach that covers all areas of the organization's security needs; It involves understanding the organization's objectives, identifying potential risks, establishing security policies and procedures, developing security controls, implementing security solutions, and ensuring compliance with regulatory standards. You will be seeking for your supervisor and teammates to approve your proposal (we will do this together live during the session) before designing a stakeholder presentation and roadmap later.	

Task	Creating a well-structured proposal and getting it approved from your team is the first step towards ensuring you're using all the relevant information you've gathered to address the cybersecurity needs of the client's business. This proposal will act as a blueprint for the development and deployment of the roadmap you will later be presenting to your client. You may use the following instructions as a guide to help you: **Objective Alignment**: Begin with a clear understanding of the client's business objectives. Align these objectives with the cybersecurity measures you plan to implement. **Risk Assessment**: Detail the potential risks you've identified so far. This should include both internal and external threats. Prioritize these risks based on their potential impact and likelihood of occurrence. **Security Policies and Procedures**: Draft a clear set of security policies and procedures that need to be implemented. This should include, but is not limited to, access control measures, data protection protocols, and incident response strategies. **Security Controls**: Propose the necessary security controls to be put in place. This can range from firewall implementations, intrusion detection systems, to employee training programs. **Regulatory Compliance**: Highlight any regulatory standards the client needs to comply with and how your proposal addresses these requirements. You're encouraged to utilize any templates or tools you have at your disposal to create this proposal. Ensure your document is clear, concise, and presents a compelling case for the adoption of your cybersecurity program. Remember, the goal is not only to protect the client's business but also to ensure that they see the value in the measures you're proposing. Once your team provides you feedback, you'll have everything you need to craft a final roadmap. You Will Know You are Done When **You will know you are done when you have collaborated with your team to identify all essential areas for the cybersecurity program. Your compiled information, both from direct discussions and additional research, should be integrated into a comprehensive and cohesive document that serves as a foundational proposal for Lemonade 's cybersecurity program.**	Cybersecurity Plan Template Example [https://www.method.me/blog/cyber-security-plan-template-for-small-business/]

Requirements Gathering

These are questions to ask from Nell Crain CTO during our initial meeting to gain a comprehensive understanding of Lemonade's security needs:

Current Security Posture

1. **What existing security controls are currently in place at Lemonade? (firewalls, intrusion detection systems, data encryption)**

2. **Have you conducted any recent security assessments or penetration tests? (Provides insight into known vulnerabilities)**

3. **Does Lemonade have a dedicated IT security team, or is security managed by the broader IT team?**

4. **How are data backups and disaster recovery procedures managed?**

Data Protection

5. **What types of sensitive data does Lemonade collect and store? (customer data, financial data, claims data)**

6. **How is access to sensitive data controlled and monitored? (Ensures data isn't exposed unnecessarily)**

7. **What is Lemonade's risk tolerance for security incidents? How much disruption or data loss would be considered unacceptable?**

8. **Are there any specific data privacy regulations (e.g., PCI-DSS, HIPAA) that Lemonade needs to comply with?**

9. **How are customer passwords currently stored and managed by Lemonade?**

10. **What current regulations or compliance requirements does Lemonade need to adhere to regarding data security and privacy?**

11. How does Lemonade manage cybersecurity risks associated with third-party vendors and partners who have access to its systems or data?

AI Model Security and Data Protection

12. Can you describe the security architecture surrounding the AI model and its training data? (Highlights potential vulnerabilities)

13. Can you provide a high-level overview of the AI model infrastructure? (data storage, access controls, model training process)

14. Can you elaborate on the infrastructure and data handling processes for Lemonade's AI model?

15. Are there any specific security concerns you have regarding the AI model or its training data?

16. Have you considered any specific security risks associated with the AI model? (bias, manipulation, data poisoning)

Business Continuity and Incident Response

17. What are Lemonade's biggest security concerns from a business perspective? (data breaches, ransomware attacks, reputational damage)

18. What are the top security priorities for Lemonade in the coming year?

19. What is Lemonade's risk tolerance for security incidents? (Guides prioritization of security controls)

20. Does Lemonade have any plans for expansion or integration with new technologies in the near future? (cloud migration, new partnerships)

21. Are there any upcoming projects or IT initiatives that could impact the security landscape? (Ensures the program can adapt to future changes)

22. **Does Lemonade have a documented incident response plan? (Essential for quickly addressing security breaches)**

23. **How are employees currently trained on cybersecurity best practices? (Helps identify potential gaps in security awareness)**

Budget

24. **Does Lemonade have a designated budget for cybersecurity initiatives?**

25. **What are Lemonade's key business objectives, and how do they relate to cybersecurity and risk management?**

26. **Which assets and data are considered most critical to Lemonade's operations, and how are they currently protected?**

27. **Could you please share with us lemonade's mission and vision, if there is any core principle that governs the brand it will be nice to know about it ?**

28. **What are the biggest cybersecurity threats facing online insurance companies like yours, and how do you propose to mitigate these risks?**

29. **Has Lemonade experienced any security incidents in the past (data breaches, attempted attacks)? If so, what were the lessons learned?**