Playbooks and Escalation

Reading

45m

Status | Incomplete

Introduction

A Cyber Security playbook is a document that combines an organization's IR plan with a business continuity plan to describe in detail what actions need to take place when data loss occurs. The playbook is designed to guide your team through a cyber incident from initial discovery to preventing a recurrence.

There are three important readings below for you to review. The goal of these readings is to assist you in understanding that IR plans and playbooks, though often unique in detail across organizations and business sectors, often contain similar tasks and connections.

As you develop your own plans, do not forget that you are not reinventing the wheel, but rather building on best practices learned and incorporated in the real world.

Required Readings

Required Reading #1

In the first reading, **The Security Playbook for Information System Solutions** by the Treasury Board of Canada Secretariat, you will cover in some detail a more formalized methodology for the creation of a playbook in an organization. This reading will allow you to take and apply your knowledge of stakeholders and incidents and create a playbook.

While reviewing this resource, please note the following:

- The focus/example is on software information system solutions being deployed in cloud environments. The thought process being introduced however can be applied into any security context.
- Think about how the information provided could be applied in a more generic context.

> Read the following with the two points above in mind - The Security Playbook for Information System Solution.

Be prepared to discuss stakeholders identified and their roles. Of particular importance is the list of possible stakeholders given.

This playbook is to be used by individuals who act in the following roles and participate in the project activities outlined in this playbook:

- The product owner
- The authorizer (if different than the product owner)
- The project team lead
- The architecture owner
- The security architecture owner (if different than the architecture owner)
- Project team members
- The security assessor
- The operations manager

Reflection - given your previous readings and work on stakeholders, can you fit the stakeholders you identified in your company from the last unit into this list?

Reflection - did you notice that goals of this playbook show that this is to be used whenever a new project is implemented? Playbooks are not just for incidents.

How to Develop a Cyber Security Playbook

A critical aspect of defining your Cyber Security playbook strategy will involve considering the business, its goals, stakeholders, and risk tolerance and using these parameters to outline the tools and approaches that will work best for the organization and its operational and productivity requirements and goals. As you can imagine, these will vary with organization type and size, among other factors, so always keep these in mind as you think about the right-fit strategy.

Similarly, identifying and documenting who is responsible for what can vary when you begin to consider different types of organizations.

When you consider normal operations, security posture maintenance as well as during incident handling, it is important to select the right people for these roles. You would want to think about ensuring the organization's security is keeping pace with rapid changes in the business on a daily basis as well. For example, smaller, private companies that are growing rapidly would likely have smaller teams to choose these roles from. If an organization is larger and more distributed, all stakeholders and involved parties and their perspectives need to be taken into account to ensure the playbook created actually supports the success and security of the entire organization.

And as a final point to think about, consider working with a more experienced external partner to speed up or enhance the process of creating and maintaining an up-to-date and effective Cyber Security playbook.

Required Reading #2

In this reading, you will review the five steps outlined by Critical Start to creating a Cyber Security playbook for an organization.

Read the following article and pay close attention to the five steps identified - How to Develop a Cybersecurity Playbook in Five Steps.

1. Define Your Cyber Security playbook strategy
2. Define the responsible parties
3. Refine the culture
4. Measure success

5. Consider an experienced Cyber Security partner

Required Reading #3

> Read this article on good security playbooks from Axcient, and pay close attention to the four areas of recovery - 5 Critical Pieces of a Good Security Playbook

Four areas of recovery discussed:

- IR plan + business continuity plan = Cyber Security playbook
- Immediate and long-term planning
- Preventing, addressing, and recovering
- Developing your own Cyber Security playbook

> In addition, download and examine the Incident Response Plan Template and save it to your PKM for future reference and use.

Conclusion

Remember these readings as you continue to fine tune your IR plans and playbooks. When starting out in this industry you may not get a chance to affect the creation of the playbook right away, but you will be given chances to give feedback on them.

✓ Mark Completed

Previous
Recognizing an Incident

Next
Cover Letters

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W06D2

Tue Jul 30

› Lectures (1)

⌄ Work (8)

6 hrs

</> Report on Company Types and Stakeholders

- Group Share and Feedback
- Recognizing an Incident
- Playbooks and Escalation
- Cover Letters
- The Incident Escalation Process
- Incident Escalation Research
- IR Quiz

W06D2 Schedule »