CYBER CRISIS MANAGEMENT PLANNING

HOW TO REDUCE CYBER RISK AND INCREASE ORGANIZATIONAL RESILIENCE

JEFFREY DON CRUMP

ISBN EBOOK EPUB: 978-0-578-52311-8
ISBN EBOOK MOBI: 978-0-578-52312-5
ISBN PAPERBACK: 978-0-578-52310-1

Library of Congress Control Number: 2019907314

www.JeffreyDonCrump.com

This book is dedicated to my two daughters, Stephanie Brooke and Madison Nicole. I’m incredibly proud to be called their Daddio.

CONTENTS

ACKNOWLEDGMENTS

Since my career spans more than 30 years, it's difficult to identify each person who's played a role leading in my ability to write this book, but I'll do my best.

I'd like to thank my parents, CMSgt Roy Crump USAF Ret. and Diane Wisner-Schiffner, for their very different but very instrumental roles in my life.

Although I never earned the title of 'PJ', I'm thankful to the US Air Force Pararescue program (and my Bad to the Bone classmates), which taught me how to remain cool, calm, and collected in high-stress situations.

Thanks go to the US Air Force and US Marine Corps, whose world-class training provided me with much needed foundational technology and security knowledge.

I'm thankful to Victor Severin for giving me the opportunity to move out of the USAF Technical Applications Center (AFTAC) computer room and upstairs into MVS Systems Programming, where attention to detail, a focus on security, and organizational resilience were rooted and tested. It was our systems in April 1986 that supported the processing of 354 air samples from the Ukrainian nuclear accident at the Chernobyl Nuclear Power Plant, located in the former Soviet Union.

Thanks also go to the US Coast Guard for sending me to the Defense Information School (DINFOS), where my writing and crisis management skills were established. These skills were tested and refined in Florida and Alaska during oil tanker collisions and subsequent fires and oil spills, cruise ship groundings, multiple loss-of-life accidents, and large-scale joint-military exercises.

Finally, I'd like to acknowledge and thank Praveen Money for the professional support and opportunities he's provided, as well as for laying the first stone on the path to writing this book while working with me in the cyber risk practice at a Big 4 professional services company.

ABOUT THE AUTHOR

Jeffrey Don Crump is the Managing Director and Principal Consultant at Cyber Crisis Response, a service of Cyber Security Training and Consulting, LLC.

He's the course author and instructor for the Cyber Crisis Management Planning Professional (C^2MP^2™) certification. Jeffrey has served as manager at Deloitte & Touché LLP Cyber Risk Services, Program Manager of Compliance & Security for ADT Cybersecurity's Datashield Monitored Security Service, and Symantec Business Critical Services Manager. He's a veteran of the US Air Force and US Coast Guard, and his professional credentials include Certified Information Systems Security Professional (CISSP®), certified Project Management Professional (PMP®), certified ScrumMaster (CSM®), and ITIL® Foundations certified.

“

In preparing or planning for a crisis, the ability to be organizationally agile is critical because although a crisis event may initially affect one aspect of the business, ultimately the entire organization, including its reputation, may be at stake.”

Lynn Perry Wooten & Erika Hayes James

Linking Crisis Management and Leadership Competencies

1

INTRODUCTION

When a high severity cyber incident strikes an organization, the financial, operational, and reputation impacts can be significant, if not catastrophic. Organizations can reduce these risks and expedite the return to normal operations through the use of a cyber crisis management plan.

Traditional information technology incident response plans often fail to consider the cross-organizational activities that need to be performed to remain resilient when a major cyber crisis occurs, resulting in a delayed, chaotic, unstructured, and fragmented response. A cyber crisis management plan is designed to reduce these risks through careful pre-planning; therefore, developing a cyber crisis management plan requires organizations to take a holistic approach to cyber crisis planning. By proactively acting to build a cyber crisis management plan, a broader, carefully considered, integrated and validated plan can be developed to meet an organization's unique demands before the crisis strikes.

This book pulls directly from the Cyber Crisis Management Planning Professional (C^2MP^2) certification course and is designed to provide the reader and organizations the knowledge and materials needed to develop their own cyber crisis management plan.

The goal is to provide the reader with a framework of information needed to build a cyber crisis management plan (CCMP) for their organization; however, it's important to understand that the combination of the framework provided, and your customized information, only establishes a baseline to refine further. The CCMP serves as a reference resource during a cyber crisis.

Organizations can, and should, customize their plan to meet their own unique requirements. Can the cyber crisis management plan framework outlined in this book meet the needs of many organizations? Yes. Will it for your organization? That can only be determined by your organization's requirements.

The content herein is intended to get straight to the point in a clear and concise manner, while also providing well-defined templates, checklists, and other examples that may meet your organization's needs just as they're presented. Again, though, the actionable material must be directly related to your own organization's needs.

Unlike the C^{2}MP^2 course, this book won't provide an introduction to the current cyber threat landscape, since it's constantly evolving. Any current day frightening headlines, case studies, or metrics that could have been included to help build a sense of urgency to develop a cyber crisis management plan would be outdated by the time this sentence ends. As such, the book is designed for readers and organizations risk aware enough and proactive enough not to require scare tactics to convince them that taking a more holistic approach to cyber crisis response just makes sense. If you're not sure having a cross-functional plan to manage a major cyber incident matters, just ask your cyber insurance agent, chief risk officer, chief information security officer, investors, the public, or any other stakeholder of your organization.

Developing a cyber crisis management plan takes commitment from senior leadership and a willingness to invest the time and resources needed to develop, document, and validate the plan. It is recommended organizations treat the work as you would any high-value project. An executive sponsor, leadership buy-in, and a talented project manager are essential to success. The value and effectiveness of the plan are directly related to the quality of effort put into building and maintaining it.

This book will begin by giving you a snapshot of the overall layout of the plan so you can visualize how the information will fit together. As you progress through the book, you'll be exposed to various concepts to such a sufficient degree, you'll be able to speak authoritatively as to why the information is in the plan. An effective cyber crisis management plan strikes a delicate balance between being informative and being usable.

You'll learn about the differences between a traditional information technology incident response plan and cyber crisis response management plan, as well as the anatomies of a cyber attack and cyber crisis response, so you can gain an appreciation for the different flows and activities within each. We'll work on developing impact categories, severity criteria, scales, and scores, which are designed to add an objective view of the incident's impact. We'll dig into various teams, roles, and responsibilities, as well as working groups.

Detailed functional incident response

plans, and the integration of the functional incident response plans into the overall response process flow, are essential to providing both high-level and granular visibility into the activities being performed throughout the crisis response. And we'll address response logistics, plan ownership and governance, and wrap up with a wide range of valuable templates and checklists.

Once the plan is framed up, we'll look at the project management aspects so you can successfully execute a project to develop a cyber crisis management plan.

The final part of the book will focus on training (your organization on your plan) and the best practices for planning and executing tabletop exercises designed to validate and optimize/improve the plan.

As you can easily deduce, there's a lot of information needed in a cyber crisis management plan; however, for it to be usable in a crisis situation, the plan needs to be structured in such a way that someone completely unfamiliar with it would be able to understand clearly what the purpose of the plan is, who the key people and groups involved in the response are, a summary of what the groups are supposed to do, and the overall logistics—all within the first few pages. The supporting detailed information can be referenced in the appendices by the plan's users on an as-needed basis, so as not to clutter the core of the plan and make comprehension and use easier.

The following sections of the book will start with information describing the section, then there will be a 'build this' section, where you'll complete tasks in a step-by-step process. Very specific examples are provided as you're building your plan to ensure you remain on the right track and give greater context to the material. This will allow you to customize the material to meet your organization's unique needs. Also, this format will ensure you have the foundation of knowledge needed to complete the step-by-step tasks. You can take two approaches when completing the tasks:

> **Approach 1:** Quickly build a framework of the plan and finalize the details as part of a future project; or
>
> **Approach 2:** Gradually complete the tasks as part of your cyber crisis plan development project so when you complete the tasks, you'll have a cyber crisis management plan ready to be validated through tabletop exercises.

Which approach you select really is a matter of preference; no right or wrong answer exists. If you read the book and complete the activities, your organization will undoubtedly be in a much better position to manage cyber risks and increase resilience.

Let's get started.

“

In the Chinese language, the word ‘crisis’ is composed of two characters, one representing danger and the other, opportunity.”

John F. Kennedy

Speech at United Negro College Fund fundraiser
(Commonly misinterpreted as ‘danger plus opportunity’; the Chinese word wēijī translates to ‘danger at a point of juncture’.)

2

THE PLAN CORE

As stated previously, it's important to keep the core sections of the cyber crisis management plan to a minimum (e.g. 10-20 pages). Although even 10-20 pages may seem like a lot, you'll soon see the material in these early pages can be read and understood very quickly.

In its final state, your plan may extend to 50, 80, or even more than 100 pages, so it's vitally important to anticipate the immediate apprehension a reader may feel when presented with such a large document. We must remain aware of the reader's perception, because if they reject the plan, it makes adoption and institutionalization more difficult than it needs to be.

Let's take a look at what's in the core.

- Cover Page (1 page)
- Table of Contents (1-2 pages)
- Acronyms (1 page)
- How to Use this Document (1 page)
- Cyber Crisis Response (1 page)
- Response Structure (1 page)
- Response Process Flow & Logistics (4-6 pages)

COVER PAGE—The cover page should contain the document title (e.g. ACME Corp. Cyber Crisis Management Plan), an organizational logo (it makes the document more attractive and helps the reader associate the plan with a particular organization or unit), and a document classification (e.g. Confidential—Not to be disclosed to any unauthorized person or organization).

TABLE OF CONTENTS—Be sure to use the proper text headers in your word processing software when you create the various sections, to ensure your table of contents is structured correctly and easy to comprehend. It's recommended you limit the table of contents to header 1, header 2, and header 3 formatting styles. If you include other header formatting styles, the table of contents can become unwieldy and cluttered.

ACRONYMS—An acronym is an abbreviation formed from the first letters of other words and may be pronounced as a word or by the letters themselves. You can't assume everyone reading the cyber crisis management plan is familiar with the unique terms or jargon used in your organization, so it's best to include them and a definition here. In addition, we'll be introducing a new set of terms, and this section is where the reader is introduced to them.

HOW TO USE THIS DOCUMENT —This section is where the reader is told which sections of the plan he should focus on to gain the appropriate level of information specific to his role. This section also helps relieve any reader anxiety he may feel due to the size of the plan by focusing his attention only on the few parts most relevant to him.

1. CYBER CRISIS RESPONSE—In this section, we tell the reader what the cyber crisis management plan is, its purpose, a simple description of its contents, and how to handle any needed changes.

2. RESPONSE STRUCTURE—In this section, we introduce the reader to the main organization groups, roles, and persons involved in a cyber crisis response. This section should include a graphic depicting the hierarchical structure and relationship of the response teams, including reference to the leaders of the groups. This allows the reader to comprehend quickly who's involved and how the groups relate to each other.

Although we'll expand the following set of teams and roles to include Working Groups later, for now the critical teams and roles are detailed below.

The Cyber Crisis Executive Team (CCET) is comprised of select members of the Executive Committee/Board of Directors and the Senior Executive-in-Charge (SEIC). The purpose of this team is to ensure this group (or your organizational equivalent of a body that provides oversight, consultation, and direction to senior leadership) has adequate information required to interact with the full Executive Committee/ Board of Directors, as needed.

The Cyber Crisis Management Team (CCMT) is comprised of the SEIC and Executive-in-Charge (EIC). The SEIC provides senior management guidance and support to the EIC, acts as an escalation point for the EIC, and liaises with members of the CCET, as needed, for strategic direction. The EIC has full authority for tactical decision-making and oversees CCRT command and control activities throughout the incident. Working with the Lead Incident Handler (LIH), the EIC will ensure response teams have much-needed administrative support in place for meeting coordination, incident chronology tracking, decision tracking, and overall coordination of the crisis response.

The Cyber Crisis Response Team (CCRT) is comprised of the LIH and Incident Response Lead (IRL) from each of the functional groups involved in the response. The specific IRLs required will be dictated by the organization's response structure. The EIC is the authoritative decision maker for the CCRT. The LIH is responsible for ensuring the incident response is progressing in accordance with the plan, communication to internal stakeholders is timely and accurate, and all members are capturing opportunities to improve future iterations of the plan.

In addition, the LIH will communicate directly with the EIC and respective IRLs, coordinate the CCRT's activities and meetings, gather information from the teams, develop and deliver incident status updates, track the response life cycle, and ensure the team's needs are met.

The Cyber Security Incident Response Team (CSIRT) is responsible for the overall technical response to the cyber crisis. The CSIRT works with information technology and information security groups, when needed. The LIH is responsible for ensuring members of the CCRT have the current status of the technical response by liaising with the CSIRT on a regular basis.

The Cyber Crisis Support Team (CCST) provides ad-hoc assistance to the CCRT. The CCST is comprised of various units or departments within the organization that may be called on to provide specialized information to the CCMT and CCRT. Members of the CCST aren't critical to the core response, but the information they provide may prove essential, so it's important to identify them. It takes very little effort to identify these groups proactively, so it's best to address this now instead of when you're in the middle of a crisis.

3. RESPONSE PROCESS FLOW & LOGISTICS—This section not only paints a big picture of the overall crisis response process flow; it also includes logistics information so personnel can effectively work together. We'll address the requirements for this section in much greater detail over the next two chapters.

Chapter 2: Build This

STEP 1 File | New

- Using a word processing tool (e.g. Microsoft Word), create a new document
- Name your plan using the following file naming convention:
  - <Your Company Name> Cyber Crisis Management Plan DRAFT <Today's date YYYYMMDD>.
  - For example: ACME Corp Cyber Crisis Management Plan DRAFT 20190520

By using this naming convention, we're able to:

- Clearly communicate what the document is;
- Clearly communicate that the plan is a draft work in progress;
- Maintain version control by ensuring you start each day's work on the plan with a new version date; and
- Ensure we have backup versions for reference or file restoration.

STEP 2 Cover Page

- Center your organizational logo in the middle of the page
- Add a Document Header and center the name of the document, which will ensure the document's title is at the top of each page
- Add a Document Footer with the document's information classification and page number
  - **Example:** Confidential—Not to be disclosed to any unauthorized person or organization

STEP 3 Frame the Core

- Start each of the following sections on a new page.
- Acronyms

How to Use this Document

1. Cyber Crisis Response
2. Response Structure
3. Response Process Flow & Logistics

STEP 4 Table of Contents

- Add the Table of Contents on a new page after the Cover Page and before the Acronyms section.

STEP 5 Acronyms

- Create a table with two columns and 13 rows
- Highlight the top row and give it a shaded color
- Enter 'Acronym' in the first column header
  - Enter 'Description' in the second column header
  - Enter the following acronyms and descriptions in the subsequent rows:

AAR After-Action Report

BAU Business as Usual/Normal Operations

CCET Cyber Crisis Executive Team

CCIF Cyber Crisis Information Form

CCMP Cyber Crisis Management Plan (this document)

CCMT Cyber Crisis Management Team

CCRT Cyber Crisis Response Team

CCST Cyber Crisis Support Team

CSIRT Computer Security Incident Response Team

EIC Executive-in-Charge

IRL Incident Response Lead (Each functional team will have a primary and (a minimum of) one backup IRL)

LIH Lead Incident Handler

SEIC Senior Executive-in-Charge

Many of these terms will not mean much to you right now, so don't worry. We'll cover these as we get further into the book.

STEP 6 How To Use This Document

- Under the section name, enter a short paragraph to describe the purpose of this section.
- **Example:** This section provides guidance as to which sections of the CCMP a

particular role/person should read and understand to use the plan effectively. For a quick overview of the plan, refer to Section 1, Section 2, and Section 3 (Process Flow graphic), which is less than three pages of material.

- Create a Text Header 2 for 'Senior Executive-in-Charge (SEIC)'
- Create bullet points for the following:
  - Section 1, Section 2, and Section 3 (Response Process Flow graphic only)
  - Appendix C: Plan Ownership & Governance
  - Appendix D: Incident Impacts, Scales & Scores
  - Appendix E: Cyber attack and Response Anatomies
- Create a Text Header 2 for 'Executive-in-Charge (EIC) & Lead Incident Handler (LIH)'
- Create bullet points for the following:
  - Section 1, Section 2, and Section 3
  - For Reference:
    - Appendix A: Response Team Roles, Responsibilities & Contacts
    - Appendix B: Working Groups
    - Appendix F: Cyber Crisis Information Form
    - Appendix G: Lead Incident Handler (LIH) Checklist
    - Appendix H: LIH-to-EIC Email Template
    - Appendix I: EIC-to-CCRT Notification Email Template
    - Appendix J: LIH-to-CCRT Initial Meeting Email Template
    - Appendix K: Initial CCRT Meeting Agenda Template
    - Appendix L: LIH-to-CCRT Subsequent Meeting Email Template
    - Appendix L: Subsequent CCRT Meeting Agenda Template
    - Appendix M: SEIC-to-CCET Email Template
    - Appendix N: Crisis De-Activation Checklist
    - Appendix O: Incident Response Plans
- Create a Text Header 2 for 'Primary & Backup Incident Response Lead (IRL)'
  - Create bullet points for the following:
    - Section 1, Section 2, and Section 3
    - Appendix O: (The plan for your functional group)
    - For Reference:
      - *Appendix A: Response Team Roles, Responsibilities & Contacts*
      - *Appendix B: Working Groups*
      - *Appendix D: Incident Impacts, Scales & Scores*

        - *Appendix E: Cyber attack and Response Anatomies*

- ➤ Create a Text Header 2 for 'All Others'
    - Create bullet points for the following:
        - Section 1, Section 2, and Section 3 (Response Process Flow graphic only)
        - For Reference:
            - Appendix A: Response Team Roles, Responsibilities & Contacts
            - Appendix D: Incident Impacts, Scales & Scores
            - Appendix E: Cyber attack and Response Anatomies

Again, don't get caught up right now with what all of these are; we'll cover them in detail later in the book. For now, focus on the structure of the plan; you'll be able to customize it after the basic structure is built.

STEP 7 Define Plan Purpose

- ➤ In the 1. Cyber Crisis Response section, add 2-4 paragraphs to provide the reader an introduction to the CCMP

Example: "The purpose of the ACME Corp. Cyber Crisis Management Plan (CCMP) is to aid our organization in the holistic response to a major cyber incident. A major cyber incident requires a coordinated and collaborative response from the Cyber Crisis Response Team (CCRT) to reduce risk and ensure organizational resilience to cyber attacks.

"The information included in this plan serves to guide the organization and its units through a series of mandatory and optional activities throughout the cyber crisis, from the initial identification and notification of the crisis to the return to normal operation/business-as-usual (BAU).

"A high-level process flow with links to detailed activities is provided as reference. The Executive-in-Charge has the right to make adjustments to the plan on an as-needed basis during the crisis to protect the organization and manage the overall response best.

"Any gaps or issues identified in this plan will be captured as they're encountered and included in an After-Action Report (AAR) to ensure the plan is optimized, as needed."

STEP 8 Response Organization

- Using a drawing tool (e.g. Microsoft® Visio® or Microsoft® PowerPoint® Illustrations) create a graphic to depict the various teams involved in the response.

The complexity of your organization will dictate whether a consolidated response organization chart or plug & play organization chart makes sense.

In the example below (Figure 2.1), you'll see the consolidated response organization, whereby all example members of the Cyber Crisis Response Team (CCRT) represent the entirety of groups that need to be involved in the response.

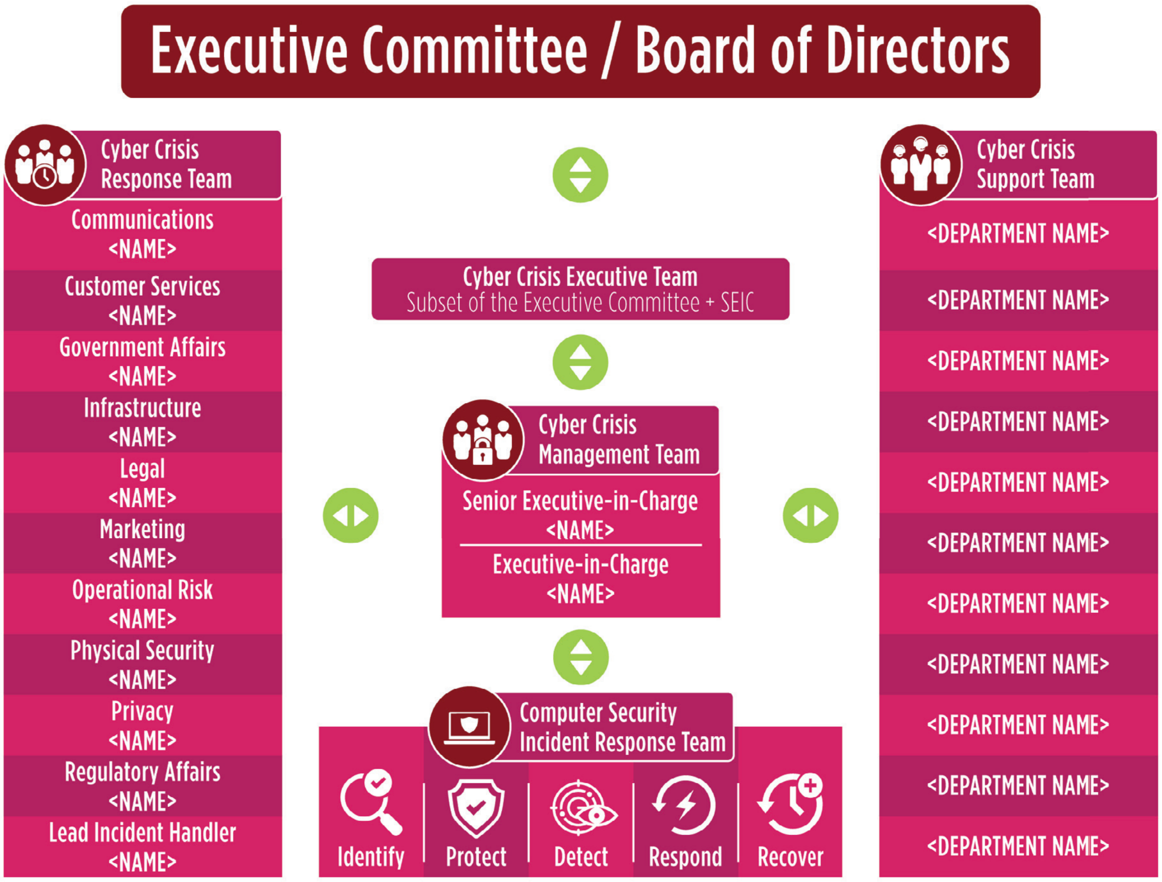
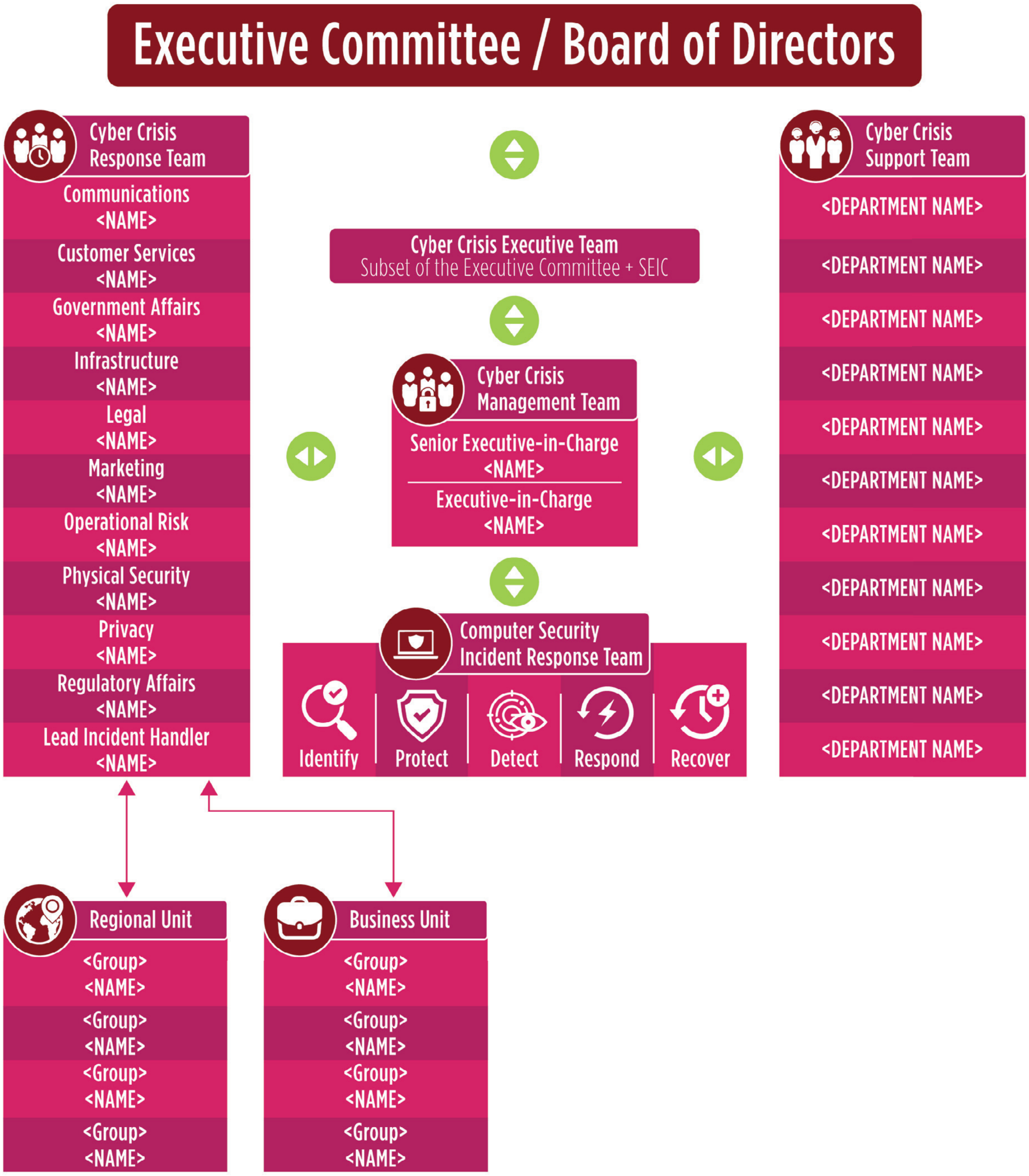


Figure 2.1: Consolidated Response Structure

In the second example (Figure 2.2), you'll see the use of plug & play units that are pulled into the core CCRT only if their unit is impacted by the cyber crisis.



Executive Committee / Board of Directors

Cyber Crisis Response Team

Communications <NAME>

Customer Services <NAME>

Government Affairs <NAME>

Infrastructure <NAME>

Legal <NAME>

Marketing <NAME>

Operational Risk <NAME>

Physical Security <NAME>

Privacy <NAME>

Regulatory Affairs <NAME>

Lead Incident Handler <NAME>

Cyber Crisis Executive Team
Subset of the Executive Committee + SEIC

Cyber Crisis Management Team

Senior Executive-in-Charge <NAME>

Executive-in-Charge <NAME>

Computer Security Incident Response Team

Identify Protect Detect Respond Recover

Cyber Crisis Support Team

<DEPARTMENT NAME>

<DEPARTMENT NAME>

<DEPARTMENT NAME>

<DEPARTMENT NAME>

<DEPARTMENT NAME>

<DEPARTMENT NAME>

<DEPARTMENT NAME>

<DEPARTMENT NAME>

<DEPARTMENT NAME>

<DEPARTMENT NAME>

<DEPARTMENT NAME>

Regional Unit

<Group> <NAME>

<Group> <NAME>

<Group> <NAME>

<Group> <NAME>

Business Unit

<Group> <NAME>

<Group> <NAME>

<Group> <NAME>

<Group> <NAME>

Figure 2.2: Plug & Play Response Structure

If your organization is complex enough to warrant the plug & play model, it'll require the cyber crisis management plan project team to prioritize the engagement so the highest risk units are part of the first iteration of the plan development. Doing so will expedite readiness for that particular unit and ultimately help reduce risks. Additional units should be added only after the initial plan has been developed and the foundational elements have been validated through a series of tabletop war game exercises.

As expected, other organizational factors may warrant your response structure be modified (e.g. if your organization has a shared services model or if particular services are outsourced).

STEP 9 Response Structure

- Above your graphic, add 1-2 paragraphs to introduce the section.

Example: "Three core teams are activated once a major cyber incident has been declared: Cyber Crisis Management Team (CCMT), Cyber Crisis Response Team (CCRT), and Computer Security Incident Response Team (CSIRT). The SEIC will decide if other groups or individuals should be engaged at the onset.

"Note: Appendix A: Response Team Roles, Responsibilities & Contacts may be referenced for a detailed description of each group. Contact information for each of the team members is provided as well."

Congratulations! At this point, you have developed a straw man for your cyber crisis management plan and entered some very important information to help readers understand the purpose of the plan, how they should use the plan, and the structure and relationship of the various groups involved in the response.

Let's move on to learning about functional incident response plans (Chapter 3: Functional Incident Response Plans), then with that information we'll build out the final part of the plan's core by developing and adding the response process flow and response logistics information (Chapter 4: Response Process Flow & Logistics).