THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

NAVIGATING THE DIGITAL AGE

EXCERPT OF CHAPTER BY RIA THOMAS

SECOND EDITION

paloalto NETWORKS

NYSE

Navigating the Digital Age:
The Definitive Cybersecurity Guide for Directors and Officers
Second Edition
Excerpt of Chapter 20

Publisher: Palo Alto Networks

Editors: Aleksandra Miljus, Mike Perkowski, and Al Perlman. **Copy Editor:** Rupal Shah

Design and Composition: Tim Heraldo and Jeffrey Rennacker

Produced With Grateful Thanks to: Kristen Batch, Deirdre Beard, Paul Calatayud, Christopher Coccagna, Elizabeth Cockett, John Davis, Greg Day, Sean Duca, Karine Gidali, Rick Howard, Danielle Kriz, Dana Loof, Rossana Monzon, Sean Morgan, Aryn Pedowitz, Michaline Todd, Alison Varela, and Sara Verri.

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers, Second Edition is published by: Palo Alto Networks, 3000 Tannery Way,
Santa Clara, CA 95054, USA
Phone: +1 408-753-4000 | www.navigatingthedigitalage.com

First published: 2018

Cover Illustration by Tim Heraldo

Disclaimer

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers, Second Edition contains summary information about legal and regulatory aspects of cybersecurity governance and is current as of the date of its initial publication May, 2018. Although the Guide may be revised and updated at some time in the future, the publishers and authors do not have a duty to update the information contained in the Guide, and will not be liable for any failure to update such information. The publishers and authors make no representation as to the completeness or accuracy of any information contained in the Guide.

This guide is written as a general guide only. It should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided. Every effort has been made to ensure that the information in this guide is correct at the time of publication. The views expressed in this guide are those of the authors. The publishers and authors do not accept responsibility for any errors or omissions contained herein. It is your responsibility to verify any information contained in the Guide before relying upon it.

GLOBAL CYBERSECURITY EDUCATION FUND

Navigating the Digital Age, Second Edition, is published by Palo Alto Networks. As a company, alleviating the problem of cybercrime is at the heart of everything we do.

Our goal is to offer cybersecurity education and training to students of all backgrounds around the globe through the Global Cybersecurity Education Fund.

Which is why every action we take, and your readership of this book, gets us one step closer to our mission—protecting our way of life in the Digital Age.

Preface

From the Editors

Welcome to the all-new second edition of *Navigating the Digital Age.* We emphasize "all new" because none of the content in this edition is repetitive of what was written in the first edition. How could it be? The first edition was published three years ago. Welcome to the Digital Age, where three years feels like a millennium.

This edition brings together more than 50 leaders and visionaries from business, science, technology, government, academia, cybersecurity, and law enforcement. Each has contributed an exclusive chapter designed to make us think in depth about the ramifications of this digital world we are creating.

An important focus of the book is centered on doing business in the Digital Age—particularly around the need to foster a mutual understanding between technical and non-technical executives when it comes to the existential issues surrounding cybersecurity.

This book has come together in three parts. In Part 1, we focus on the future of threat and risks. Part 2 emphasizes lessons from today's world, and Part 3 is designed to help you ensure you are covered today. Each part has its own flavor and personality, reflective of its goals and purpose. Part 1 is a bit more futuristic, Part 2 a bit more experiential, and Part 3 a bit more practical. We hope you find each to be thought-provoking and valuable.

One of the pleasant surprises we discovered in editing these chapters was how seamlessly and, at times, brilliantly our authors were able to connect the business and technology challenges of cybersecurity to the broader issues facing the world at large.

But, in retrospect, we probably shouldn't have been surprised. After all, what makes this book so necessary and, we hope, so compelling is the reality that digital technologies are completely embedded in every aspect of our lives. And, as you will discover in the pages ahead, we're still only at the beginning of our journey in navigating the Digital Age.

Unless otherwise stated, all $ amounts are in U.S. dollars.

Table of Contents

Part 1 – The Future of Threat and Risks

Introductions

Seizing the Opportunities, Understanding the Challenges

Why and How We Must Change Our Roles and Behaviors

How Work Requirements and Ethical Responsibilities Come Together

Part 2 – Lessons From Today's World

Introductions

Cybersecurity Awareness, Understanding, and Leadership

The Convergence and Divergence of Compliance and Cybersecurity

Part 3 – Make Sure You're Covered Today

Introductions

Language

Strategy

People

Process

Technology

Conclusion

PART 2
Lessons From Today's World

20

Beyond Compliance: The Human Element of Cyber Resilience

Ria Thomas — Partner and Global Co-Lead for Cybersecurity, Brunswick Group

Over the last several years, with the rise in massive data breaches, which lead to public outcry, governments have responded with ever-increasing regulatory requirements. The European Union's General Data Protection Regulation (GDPR), which came into enforcement on May 25, 2018, may be the most well-known of these governmental efforts.

The need for such a regulation and the complex efforts it took to address its requirements highlighted how poorly prepared companies can be when looking at the issues surrounding their obligations. And yet, GDPR only addresses one significant aspect of cyber risk to a company—the potential loss of individuals' data and its privacy, which the company has a duty to protect.

Like GDPR, most cyber regulations are created to protect society from behavior that could cause negative impacts. These regulations are likely rooted in the experience of previous attacks and may not extend to other issues until there is enough widespread acknowledgement of the need for certain practices to be modified.

As such, compliance with regulation alone cannot cover the business risks and impacts a company faces from cyberattacks.

Businesses can move beyond compliance by striving to understand the human element. By changing corporate cultures and altering behaviors, they can take proper steps to ensure they are taking the right approach to cybersecurity and, consequently, protect their valuation and hard-earned reputation.

For the leaders of any organization, whether you are part of the executive management team or the board, the path to better cybersecurity extends to the people, processes, technologies, and cultures you put in place, regardless of whether a regulation requires it.

Being prepared is not merely about achieving or even maintaining compliance; it is about adopting a cybersecurity culture that ensures the people in your organization are ready to deal with any eventuality, whenever it may occur. And that includes you. Active board and executive committee-level ownership of cybersecurity and its enterprise-wide prioritization are essential for comprehensive, company-wide cyber resilience.

Understanding the Human Element of Cyber Resilience

In today's business, cybersecurity is a combined human and systems challenge that requires the close attention and involvement of the company's senior leadership. First, it is critical to undertake the necessary technical investments, not only to protect your company, but also to be able to demonstrate that you understood the technical risks and sought to mitigate them to the extent it was feasible.

That being said, it is important to acknowledge that cyber risks are caused by humans. And cyber prevention is managed by humans. How you work to prevent a cyberattack and how you respond to one starts with understanding who is involved. There are three general categories of players to consider when we are dealing with cybersecurity. These are:

1. **The people attacking the business.** These are the people who are out to harm your organization, whether for profit, geopolitical gain, mischief, mayhem, or any other reason. As has been discussed in other chapters within this book, the nature of these attackers is changing all the time, including their motivations and attack methods. One important point to remember: Regardless of the motivation, methodology, or attack mechanism, it is human actors who are behind the attack and whose often unpredictable actions you will need to confront.
2. **The people responding within the business.** The ability to minimize the operational, financial, and reputational impacts of a cyberattack does not rest in the hands of one individual or one group within a company. Instead, it requires both vertical and horizontal leadership and coordination.

   Board members set the governance strategy and hold the keys to accountability in terms of how the company leadership prepares and responds to a cyber crisis. Executive leaders build the culture, make key investments, and ensure a crisis structure that integrates the company's information-sharing and response coordination; they also undertake critical strategic decisions during a cyber crisis. Neither the board nor the executive committee can be successful, however, without the people who work under them. These individuals are the ones on whom they need to rely to obtain an accurate, timely understanding of the technical, operational, financial, and reputational implications of the attack. They are drawn from across the business and should include cyber/IT, legal, human resources, corporate communications, government/regulatory affairs, et al.

   Part of being prepared means knowing that the entire organization needs to come together, not only to create an integrated picture of the business impacts but also to coordinate a response that will minimize the potential fallout. It requires that each person understands their role, responsibilities, and what is expected of them during a cyber crisis.
3. **The people impacted by the cyberattack on the business.** A key element to maintaining resilience in the face of a cyberattack is demonstrating that senior leadership understands the human impact of the cyberattack on those to whom it has an obligation.

These are not only the people inside your organization, but outside it as well.

If an attack impacts your infrastructure, you may not be able to provide services to your customers. If you are in a critical industry, such as banking, utilities, healthcare, or transportation, the results can be devastating to individuals who rely on those services. If you are in retail or another customer-facing industry, you can lose sales and customer goodwill. If you suffer a data breach, important personal records of customers could be exposed on the Dark Web, creating risk of identity theft, financial loss, and other consequences.

It is critical to understand that you, the company leadership, are making decisions based not just on what is best for your bottom-line. Rather, you should demonstrate you are minimizing and mitigating the impacts on the people directly affected by the cyberattack; this focus will ultimately affect your bottom line.

Building a "Beyond Compliance" Corporate Cyber Culture

Adopting additional measures to ensure compliance with a regulation can be a critical turning point in how a company addresses a specific cyber risk that the regulation seeks to address.

It is imperative, however, not to assume that compliance alone will protect your business from the wide-ranging ramifications of cyberattacks. Instead, the focus should be on each aspect of the human element described above.

Given the range of evolving cyber threats and risks, the first step for company leaders, whether in the boardroom or the executive suite, is to take the time to understand the threat environment for your organization, including the potential business risk and the potential business impact.

Assessing the threat environment involves more than the technical risks. It also requires you to understand how your various strategic business decisions may be increasing your risk of a cyberattack. For example, as you enter into a new business venture, acquisition or partnership, or you move into a new international market or build critical intellectual property around a cutting-edge technology, who are the human beings interested in attacking your business? What could they be seeking to achieve? What kind of damage can they cause?

The next step is to engage with all of the key members of your organization who will need to create an integrated understanding of the impacts and who will be required to come together to help coordinate the corporate-wide response. Are they aware of leadership's expectations of them during a cyber crisis? Do they know their roles and responsibilities? Will the existing crisis structure, whether formal or informal, be able to handle a multi-faceted cyberattack?

As part of the pre-cyber crisis preparation, it is also critical that company leadership invest in raising employee awareness, not only of cyber risks but also of the behavior that may be expected of them to protect the organization from cyber threats.

The above measures will allow you to stay resilient in a cyber crisis because the human beings you need to rely on to minimize the long-term impacts, especially to your reputation, are already within your organization. Creating a corporate-wide, cyber-resilient culture requires not only their active engagement and participation, but their buy-in.

Finally, during a cyber crisis, you should take into account the spirit of most regulations: How do you ensure that your priority is understood to be the human beings who are most impacted by the attack on your business? These are not only your customers, partners, and your employees, but also the general public. What are the principles by which you lead your company through the cyber crisis? Are they protecting your business operations and valuation? Or do your actions and words convey that you have understood the weight of the trust that has been placed in your business by the human beings on the other side of the crisis?

It is possible that a cyberattack on your business and its ramifications will not fall within the confines of a particular regulation, such as GDPR, but it may still have an enormous impact on the public. How the public reacts has little to do with compliance and everything to do with perception: Did you do everything you were supposed to do? Put more succinctly: Did you do the right thing, even if you were not required by law to do so?

To accomplish this, you need to ensure that you have the right strategies and policies in place to reflect that you have planned for and thought about these things *before* the incident took place. This preparedness approach is where the right culture can leverage institutional muscle memory. You will not be able to think everything through in advance, but if your core group understands their roles and responsibilities, you are in a much better position to do the right thing and shape public perception in a positive way.

Conclusion

Compliance with regulations alone does not ensure cyber resilience. Instead, your organization's ability to overcome the myriad impacts of a cyber crisis starts with understanding your cyber risks, the potential impacts, and the measures you need to put into place in order to maintain your ability to steer through the crisis. Those efforts cannot be successful without taking into account the human beings that form the core of the threat, the response, or the impact.

IMPLEMENTING A CORPORATE-WIDE CYBER RESILIENCE APPROACH

How do you ensure that your organizational cybersecurity culture goes beyond compliance into resilience? Here are additional suggestions and questions to consider for each of these critical aspects of your cyber resilience approach:

1. **Assessing risks of a cyberattack:**
   - Do you have a comprehensive understanding of the business risks you face from the technical, operational, and strategic threats posed by a cyberattack?
   - How would you define a worst-case scenario, e.g., timeline of acceptable operational disruption; type of market impact; level of government scrutiny; public/media attention?

- Are you addressing challenges regarding a possible lack of skilled cybersecurity staff?

2. **Understanding the impacts of a cyberattack:**
    - What processes do you have in place to understand the multiple impacts of a cyberattack across corporate units or of one that is combined with physical attacks?
    - How do you prioritize or reconcile conflicting national or international regulatory requirements, such as GDPR?
    - What liabilities and obligations exist to internal and external stakeholders, including employees, customers, partners, and regulators?
    - Do you have a program in place to assess the impacts of an attack by an aggrieved employee with access to your business and customer critical data or your network?

3. **Planning and executing your cyber crisis response:**
    - Is there a corporate-wide incident management plan in place for a range of cyberattacks that accounts for your cyber risks?
    - Do senior leaders across the organization understand their roles and responsibilities? Is there a structure of support under them to ensure they have the information they need in a timely manner?
    - Is there an employee awareness program in place to increase employees' understanding of cyber threats and the need for good cybersecurity practices, including those relating to their social media activity?
    - Who are the internal and external stakeholders you need to notify and/or alert? How will you prioritize?
    - How do you deconflict information shared by your business units and coordinate how much information is being shared with whom and when?

4. **Communicating with internal and external stakeholders:**
    - Does your strategic communications plan include prescripted, pre-authorized messaging related to the cyberattack scenarios that are relevant to your cyber risks?
    - Is there a process by which you notify employees and external stakeholders, especially if key methods—phones, email—become corrupted or disrupted because of a cyberattack?
    - Who is the "face" of your company during a significant cyberattack? Have they been media-trained? Are they ready to lead by example?