THE CYBERSECURITY SOCIAL CONTRACT

IMPLEMENTING A MARKET-BASED MODEL FOR CYBERSECURITY

INTERNET SECURITY ALLIANCE
Foreword

In less than a generation, we have gone from the industrial age to the digital age. The Internet, and the digital technologies associated with it, are arguably the most influential inventions in the history of humankind. Digital technologies affect virtually every aspect of our lives from our physiology to our identity, how we develop and manage relationships, the meaning of core values such as privacy, and many of the assumptions we have long held about national issues such as economics and national defense.

Unfortunately, governance has not kept pace with the digital revolution. The digital revolution has come upon us so quickly, so easily, and in many respects, so pleasurably that we have not devoted the time and effort necessary to understand how to manage the digital world.

It’s hard to underestimate the costs of failing to manage the risk of digitalization. Numerous doomsday speculations envisioning critical infrastructure going dark or defense weaponry misfiring because of cyberattack have been well chronicled elsewhere. Recent sophisticated economic modeling shows that the difference between establishing an Internet characterized by strong cybersecurity and one in which cyberattackers continue to enjoy their ability to compromise the system is a staggering loss of $90 trillion by 2030.

As awareness of the cyber threat has grown, public and private policy makers have been subjected to a cacophony of ideas, prescriptions, technologies, and advice. All too often this massive information overload has led to confusion and uncertainty with a resulting paralysis of action just when we need clearheaded and decisive policy.

This book is an attempt to provide a coherent and systemic framework for collaborative action. Advanced technology needs to be integrated with practical economics and thoughtful public policy to
create a sustainable system of cybersecurity. Our hope is to provide a clear path the next president and Congress can follow in collaboration with the private sector. The proposals provided build on conceptual consensus that has already been embraced by both political parties and the private sector. However, this volume moves this consensus from concepts onward to strategy and implementation.

Our goals are to crystallize the problem, recognize areas of progress, and identify gaps that need to be filled.

The book is separated into three sections. The first two chapters provide a snapshot of the current problem and brief history of US public policy, including why traditional approaches are a poor fit for this unique problem and how a new model—the Cybersecurity Social Contract—has evolved. The second chapter offers a series of high-level recommendations, many of which receive more detailed treatment as they are applied in the subsequent sections.

The second section encompasses eight chapters. Each chapter covers cybersecurity issues from the perspective of individual economic sectors and outlines pragmatic steps to improve cybersecurity in these specific sectors. Each of these chapters discusses what makes the sector unique, what challenges the authors see for the next administration and Congress, and offers a set of specific policy recommendations tailored to that specific sector. Each expert has been charged with answering the question: If you had thirty minutes with the next president of the United States to advise on cybersecurity, what would you say?

The recommendations occur at three levels of abstraction. Since one of the major impacts a new president can have is to set tone, direction, and prioritization, some recommendations focus on that higher level of abstraction (e.g., we need to act with greater urgency and spend more money). Other recommendations are at a systemic level, such as government needs to get hold of the metastasizing bureaucracy strangling effective action and adapt to more modern approaches to supply-chain
management, workforce education, and auditing. Still other recommendations are at the concrete operational policy level, such as specific recommendations to develop metrics for cybersecurity programs, to altering clearance processes, and even altering Medicare reimbursement.

The final section addresses a set of seven crosscutting issues that government and industry need to face irrespective of any unique sector. These chapters address how corporate boards understand the cyber risk, how the auditing community is adapting to the cyber risk, how organizations can structure themselves to best address the cyber risk, what role insurance can play in transferring cyber risk as well as addressing issues such as workforce development, privacy, and the best way to manage the public-private partnerships called for in the social contract.

The goal is to provide a coherent, comprehensive, credible policy framework for government and industry. The volume is comprehensive not only in the sense that it addresses issues and sectors not generally discussed in this field (such as agriculture, manufacturing, and auditing), as well as the usual suspect critical industry sectors, but also because it takes a comprehensive view of the problem, including economic, structural, and policy issues in addition to technical ones. The book is credible in that the chapter authors are individuals who do cybersecurity as their day (and often their night) job. It follows a thought-out conceptual framework—a theory—already intellectually accepted by both industry and government (bipartisan) and adapts it to the implementation level.

The reader may note some redundancies across the chapters. There are several reasons for this. One reason is that good ideas in one sector may well be good ideas in a different sector. However, more importantly, the book is designed so that it can be read in modules. With a prime audience intended to be policy makers, it is understood that readers interested in financial services may not be interested in the defense chapter even if similar ideas are proposed in each.
We are hopeful that by laying out this theory and demonstrating how it may be implemented in multiple domains of the problem, we will make it easier for government and industry to enact policies and procedures to more quickly address a growing problem of cyber insecurity.

Endnotes
Contents

Foreword

Section I: A Social Contract for Cybersecurity

Chapter 1: A Brief History of the Cybersecurity Problem and Policies That Have Attempted to Address It

Larry Clinton, President and CEO, Internet Security Alliance

Chapter 2: A Twelve-Step Program for Implementing the Cybersecurity Social Contract

Larry Clinton, President and CEO, Internet Security Alliance

Section II: Cybersecurity in Industry Sectors

Chapter 3: Cybersecurity in the Defense Industrial Base

Jeff Brown, Vice President and Chief Information Security Officer, Raytheon

JR Williamson, Director and Deputy Chief Information Security Officer, Northrop Grumman

Chapter 4: Cybersecurity in the Healthcare Industry
Dustin Wilcox, Vice President and Chief Information Security Officer, Centene

Chapter 5: Cybersecurity in the Banking and Financial Sector

Daniel Crisp, Chief Information Risk Officer and Head of Technology Compliance, BNY Mellon

Larry Trittschuh, Threat and Vulnerability Leader, Synchrony Financial

Gary McAlum, Chief Security Officer and Senior Vice President, USAA

Chapter 6: Cybersecurity in the Power Utility Sector

Scott DePasquale, Chairman and CEO, Utilidata

Chapter 7: Cybersecurity and the Information Technology Industry

Art Coviello Jr., Executive Chairman (Retired), RSA

Chapter 8: Cybersecurity in Telecommunications

Richard Spearman, Group Corporate Security Director, Vodafone

Chapter 9: Winning the Cyber-Talent War: Strategies to Enhance Cybersecurity Workforce Development

Dr. David Brumley, Professor of Electrical and Computer Engineering and Director of Carnegie Mellon's CyLab Security and Privacy Institute
Chapter 10: Cybersecurity in the Manufacturing Sector

Brian Raymond, Director of Innovation Policy, National Association of Manufacturers

Chapter 11: Cybersecurity in the Food and Agriculture Sector

Dr. Robert Zandoli, Global Chief Information Security Officer, Bunge Limited

Section III: Crosscutting Issues in Cybersecurity

Chapter 12: The Evolving Role of Boards in Cyber-Risk Oversight

Ken Daly, CEO, National Association of Corporate Directors

Larry Clinton, President and CEO, Internet Security Alliance

Chapter 13: Cybersecurity Assurance: A Comprehensive Approach

Center for Audit Quality

Chapter 14: The Role of Cyber Insurance in Promoting Cybersecurity

Tracie Grella, Head of Cyber Risk Insurance, AIG

Chapter 15: Deploying a Voluntary Cyber-Resilience Program: A Strategic Imperative

Andrea Bonime-Blanc, JD/PhD, CEO, GEC Risk Advisory


Chapter 16: The Digital Equilibrium Project: Balancing Cybersecurity and Privacy

James Kaplan, Partner, McKinsey & Co

Salim Hasham, Partner, McKinsey & Co

Chris Rezek, Senior Expert, McKinsey & Co

Chapter 17: Best Practices for Cybersecurity Public-Private Partnerships

Larry Clinton, President and CEO, Internet Security Alliance

Appendix A: Ten Cybersecurity Items for the President’s First One Hundred Days

Appendix B: Briefing Memos
Chapter 15

Deploying a Voluntary Cyber-Resilience Program: A Strategic Imperative

Andrea Bonime-Blanc, JD/PhD, CEO, GEC Risk Advisory

A Holistic Approach to Corporate Cyber Resilience

This chapter makes the case that to be cyber resilient, businesses of any kind, shape, or form should design, develop, and implement a voluntary internal cyber governance, risk, and compliance/culture program (“Cyber-GRC program”).

Developing and adopting a Cyber-GRC program will allow a company to gain better and more sustainable cyber resilience, benefitting the entity itself (in terms of preparedness, crisis management and business continuity), its key stakeholders (in terms of value preservation and creation), its communities and society as a whole (in terms of safety and protection of people and assets), and regulators (who will have fewer cases of enforcement). A holistic, strategic approach to corporate cyber resilience developed voluntarily, internally, and customized to the specific needs of a company also obviates the need for unnecessary, bureaucratic, inapplicable, or otherwise extraneous and costly laws and regulations. Figure 15.1 depicts a holistic approach to Cyber-GRC.
The cyber-resilient company will have the following three general categories of Cyber-GRC in place:

1. **Cyber governance** is a framework that includes oversight, strategy, and a plan for implementation of the overall company approach and philosophy on cybersecurity as articulated by the board, the C-suite, and the top cyber-focused executives. Cyber governance is the first and most important step that a company should take as it develops its overall posture, strategy and tactics necessary to address the company’s specific cyber-threat profile.

2. **Cyber-risk management** integrated with an enterprise-risk-management system refers to the system of risk management in place for managing cyber risk, a leading example of which is the NIST Cybersecurity Framework. Having a robust and evolved risk-management system that addresses the cyber risks applicable to a particular company and its sector, footprint, products,
services, and “crown jewels” is a necessary second step in building cyber resilience, which will help to determine the best shape for the third major element, the Cyber-GRC program.

3. **Cyber Culture** zeroes in on how the cyber-governance strategy and risk-management framework can best be implemented throughout the organization and at the front lines, especially focusing on people (employees and third parties), and providing them with the practical and cultural tools and resources necessary to meet the particular cyber challenges the company faces.

Most mature or advanced companies who are proactively addressing their cybersecurity already have some form of cyber governance in place as well as cyber-risk management, although in many cases even these elements are still under development given the relatively novel, superchallenging, and constantly changing nature of the cyber threat. Some may also have identified but have not yet fully integrated into their overall Cyber-GRC culture. Companies that fully integrate these three elements into their cyber-resilience strategy will become more robust and capable of managing crises.

**A Robust Cyber-Resilient Culture Trumps the Law**

There is, however, another great benefit to the deployment of an internal Cyber-GRC program. By building internal resilience into the governance, risk, and culture of your company—people and assets—there is less need for regulatory and government involvement in legislating the minutiae of cyber management at the company level. This is a win-win for both the private and public sectors as companies pursue what is truly useful for their particular sector, footprint, and overall profile, and regulators don’t spend time and taxpayer money spinning unnecessary and expensive wheels trying to regulate too much or the wrong things at the expense of effectiveness.

A key postulate is that if companies build robust cyber resilience, the need for additional and potentially costly and ineffective laws and regulations will be obviated. Part of the purpose of this chapter is to
show both private- and public-sector decision makers what a robust, voluntary Cyber-GRC program looks like so that each can identify and understand when a company has such a profile when and if things go wrong from a cybersecurity standpoint.

I use a powerful precedent to the idea of a voluntary internal Cyber-GRC program: the experience of companies over the past three decades in building effective ethics and compliance programs to meet their legal, compliance, and integrity risks. Drawing heavily on this enlightening precedent, later sections provide the case for more internal resilience and less external regulation through the deployment of a Cyber-GRC program and a roadmap to accomplish more holistic, strategic overall cyber resilience.

A Paradigm from Another Time: The Defense Industry Initiative and the Rise of the Effective E&C Program

Introduction

The paradigm is the result of a period of decades of collaboration between companies, professional associations, research and academic sources, and, yes, lessons learned from challenging examples, mistakes, and scandals unfolding in the marketplace with concomitant waves of prosecutions, legislation, and regulation. In this chapter we refer to this paradigm as the “E&C paradigm.”

However, an important distinction needs to be made upfront on the use of this paradigm. As cyber threats have increased exponentially over the past few years, it is important to note that cyber risk is quite different from the average ethics and compliance challenge. Cyber mostly happens not because of “bad actors,” negligent or reckless leaders, a toxic culture or pervasive unethical conduct. Cyber events happen mainly because of the barrage of technological, geopolitical, and economic changes that have so quickly evolved and the exponential growth of the cyber underworld that is overwhelming the global marketplace.
In other words, unlike ethics and compliance challenges, companies do not fully control cyber challenges—and because of the nature of the cyber threat, neither should corporations be held as being fully responsible for it. Cybersecurity is a challenge that requires a broad set of solutions and one of them is the adoption by all companies of a customized, voluntary Cyber-GRC program that will in turn obviate the need for unnecessary and largely inapplicable and ineffective new laws and regulations.

The Defense Industry Initiative

The origins of the E&C paradigm can be traced back to the launch of the Defense Industry Initiative in 1985. The DII emerged in the wake of several waves of corruption and fraud involving the defense industry, starting with the foreign bribery scandals of the 1970s that led up to the adoption of the Foreign Corrupt Practices Act of 1977 and the defense procurement fraud cases of the early 1980s (involving many of the same defense industry companies) that triggered congressional investigations and the creation in 1985 of the Packard Commission to investigate fraud in the defense industry.

While the Packard Commission investigated what appeared to be industry-wide fraud and abuse, Jack Welch, then CEO and chairman of General Electric, started an industry initiative—eventually named the DII—calling for the collaboration of eighteen other major defense contractor CEOs. The DII developed in tandem with the Packard Commission investigation to such a point that when the commission report was published in 1986, the DII principles (the defense industry’s voluntary code of conduct program to establish internal guidelines for each company to address and promote ethical and compliant behaviors within their companies) were attached as an exhibit to the report.

Chapter four of the Packard Commission report starts with this statement: “In our view, major improvements in contractor self-governance are essential,” underlining the need for voluntary change to meet the ethical and legal challenges of the industry. The report then lists five key components of
defense contractor self-governance, or what would eventually be considered elements of an effective E&C program:

1. Creating well-defined risk-based codes of conduct.
2. Developing a system that tracks and vets conflicts of interest.
3. Developing an employee instructional and communications system.
4. A system to monitor compliance and internal controls.
5. An independent audit committee.

Over time, the DII became both the harbinger and a major contributor to the larger debate about, and development of, the E&C paradigm. The DII was the principal precursor to a key governmental initiative—Chapter Eight of the United States Sentencing Guidelines, first published in 1991 and amended several times since then. The USSG is a hybrid animal. It is neither law nor regulation but provides a series of guidelines for prosecutors and judges to help them determine whether a company with an underlying civil or criminal allegation or conviction has an effective E&C program. If a company is found to have such a program, it can derive very substantial financial and reputational benefits (lower or no fines, deferred or no prosecution, less or no media and social-media-driven brand damage, etc.).

The Evolution of the E&C Paradigm

Over the decades following the creation of the DII and the USSG, a number of other factors both nationally and internationally have helped to sculpt what is increasingly acknowledged to be an “effective” E&C program within the private and public sectors, with board directors and corporate executives on the one hand and prosecutors, legislators, and regulators on the other, acknowledging their importance in determining whether a company is acting with or without integrity and whether or not it deserves investigation, prosecution, or other legal sanction.

Among the key trends over the past two decades are the following:
• **Industry codes**: market-based code of conduct initiatives in the healthcare, pharmaceutical, electrical, extractive, and other industry sectors, nationally and internationally.

• **NGOs**: the long-term lobbying, pressure, and research of international nongovernmental organization Transparency International being one of the first and still leading examples of such an NGO working against corruption worldwide.

• **International conventions**: the passage of international anticorruption conventions, the first and most notable of which was the Organization of Economic Cooperation and Development Anti-Bribery and Anti-Corruption Convention of 1997.

• **High court decisions**: the first and most important of which was the Caremark decision of 1996 in which the Delaware Court of Chancery made a landmark decision expanding the duty of care of boards of directors in overseeing ethics and compliance programs.

• **Regional and national initiatives**: regional anticorruption conventions and agreements (including, notably, the United Nations Global Anti-Corruption Convention, similar regional anticorruption initiatives in Latin America, Africa and Asia, as well as programs at the World Bank and similar institutions).

• **Professional associations and think tanks**: the tireless work of professional and corporate member associations in helping to develop these ethics and compliance national and global standards also requires much acknowledgment.

These and other developments have had a major effect on the global debate and development of what we could now call a global E&C paradigm. While there was always a to-and-fro between the private sector and the public sector on the development of E&C programs, most governmental initiatives (other than anticorruption laws) have focused on providing guidelines to the private sector.

This has included, most notably, in the United States in the last few years, the Department of Justice and Securities and Exchange Commission soliciting private-sector compliance officer input, listening to,
analyzing, and incorporating what the private sector had developed voluntarily in terms of E&C programs. In these cases, the DOJ and SEC have adopted the private sector’s best practices E&C paradigm to the point of even hiring a private-sector compliance officer to review the compliance programs of companies under investigation or prosecution to determine whether or not they are “effective” and whether or not such companies deserve a break from the full weight of the law.\textsuperscript{viii}

The Emergence of the USSG

It should be emphasized that, at the time of the creation of the DII in mid-1986, there were no other notable incentives in place for the creation of an internal system of business ethics or governance other than the existence of specific federal, state, and local laws forbidding all manner of wrongdoing. Constructive incentives to do the right thing from a preventative compliance standpoint did not exist until the USSG indirectly created such a framework through Chapter Eight several years later.\textsuperscript{ix} When adopted in 1991, Chapter Eight of the sentencing guidelines provided the first cross-industry set of government incentives for corporate wrongdoers or potential wrongdoers to create an internal system of business conduct and compliance.

In essence, Chapter Eight mimics many of the tenets of the DII principles. Table 15.1 summarizes the many areas of equivalency and similarity of the respective elements of a sound E&C program as set forth under each document.

\begin{table}[h]
\centering
\begin{tabular}{|l|}
\hline
\textbf{Table 15.1} \\
\hline
\hline
\end{tabular}
\end{table}
<table>
<thead>
<tr>
<th>DII Principle&lt;sup&gt;x&lt;/sup&gt;</th>
<th>Chapter Eight of the US Sentencing Guidelines&lt;sup&gt;xi&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1:</td>
<td>Code of conduct and system of policies</td>
</tr>
<tr>
<td>Written code of business ethics and conduct</td>
<td></td>
</tr>
<tr>
<td>Principle 2:</td>
<td>Training and communications programs</td>
</tr>
<tr>
<td>Employees’ ethical responsibilities</td>
<td></td>
</tr>
<tr>
<td>Principle 3:</td>
<td>Anonymous and other reporting without fear of retaliation</td>
</tr>
<tr>
<td>Corporate responsibility to employees</td>
<td></td>
</tr>
<tr>
<td>Principle 4:</td>
<td>Internal compliance risk assessments, monitoring,</td>
</tr>
<tr>
<td>Corporate responsibility to the government</td>
<td>and auditing</td>
</tr>
<tr>
<td>Principle 5:</td>
<td></td>
</tr>
<tr>
<td>Corporate responsibility to the defense industry</td>
<td></td>
</tr>
<tr>
<td>Principle 6:</td>
<td>Effective, comprehensive, and fair system of</td>
</tr>
<tr>
<td>Public accountability</td>
<td>internal discipline</td>
</tr>
<tr>
<td></td>
<td>Delegation of approval authority (system of</td>
</tr>
<tr>
<td></td>
<td>internal controls)</td>
</tr>
</tbody>
</table>
The Emergence of a Global E&C Paradigm

Fast forwarding over the next two decades, it is possible to articulate the key elements of an “effective” E&C program, or what we are calling the E&C paradigm. Figure 15.2 provides a breakdown of the nine elements of an effective E&C program as it exists as of now.xii

Figure 15.2.

<table>
<thead>
<tr>
<th>The Elements of an Effective Ethics and Compliance Program</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E&amp;C Risk Assessment</strong></td>
</tr>
<tr>
<td><strong>Code &amp; Policies</strong></td>
</tr>
<tr>
<td><strong>CECO Resources</strong></td>
</tr>
<tr>
<td><strong>Board and C-Suite Access</strong></td>
</tr>
<tr>
<td><strong>Training and Communications</strong></td>
</tr>
<tr>
<td><strong>Internal Controls Alignment</strong></td>
</tr>
<tr>
<td><strong>Helpline/Hotline System</strong></td>
</tr>
<tr>
<td><strong>Consistent Discipline</strong></td>
</tr>
<tr>
<td><strong>Audit, Monitor, and Evaluate</strong></td>
</tr>
</tbody>
</table>
The most recent salvo in this long ongoing private-public debate was just issued in mid-2016 by the Ethics and Compliance Initiative (ECI, successor to both the ECOA and the ERC), consisting of a more succinct but powerful series of principles as follows:

- **Principle 1:** ethics and compliance is central to business strategy.
- **Principle 2:** ethics and compliance risks are identified, owned, managed, and mitigated.
- **Principle 3:** leaders at all levels across the organization build and sustain a culture of integrity.
- **Principle 4:** the organization encourages, protects, and values the reporting of concerns and suspected wrongdoing.
- **Principle 5:** the organization takes action and holds itself accountable when wrongdoing occurs.\[xiii\]

**Building and Deploying a Voluntary and Effective Cyber-GRC Program: A Roadmap**

What can we learn from the evolution and emergence of the E&C paradigm that might be applicable to the creation of a robust and voluntary Cyber-GRC program within companies? As we articulated at the beginning of this chapter, there are three basic elements of a strong cyber-resilience or GRC Program: governance, risk management, and culture.

**Risk Governance**

This means that the company board, C-suite, and top enterprise risk and technology managers are all on the same page about how strategic risk, including cyber risk, is handled at the company. Do they follow the strategic risk governance best practice of applying a triangular approach to key strategic risks such that:

- The board exercises effective strategic risk oversight.
• The C-suite prepares the business strategy and strategic plan taking key risks into account and providing the necessary budget, resources, and management for the company to meet these challenges.

• The key executives and management in charge of implementing the business plan and strategy are both talented and equipped with the necessary tools, budgets, and strategic guidance to accomplish the board and CEO vision.

Figure 15.3 is a depiction of the triangular cyber-risk governance approach I advocate in another piece I wrote for the Conference Board in 2015.\textsuperscript{xiv}
The ten key takeaways of the Conference Board report on “Emerging Practices in Cyber-Risk Governance” are summarized in figure 15.4 and provide a sense of some the key practices that make for a robust cyber-risk-governance deployment.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Develop a triangular governance approach to cyber risk management</td>
<td></td>
</tr>
<tr>
<td>2. Understand the reputation risk consequences to strategic cyber risk management gone wrong</td>
<td></td>
</tr>
<tr>
<td>3. Know who your cyber risk actors and stakeholders are</td>
<td></td>
</tr>
<tr>
<td>4. Have a deep understanding of the organization’s “crown jewels”</td>
<td></td>
</tr>
<tr>
<td>5. Engage in a relevant cyber risk public-private partnership</td>
<td></td>
</tr>
<tr>
<td>6. Develop a cross-disciplinary approach to cyber risk management</td>
<td></td>
</tr>
<tr>
<td>7. Develop a cross-segmental/divisional approach to cyber risk management</td>
<td></td>
</tr>
<tr>
<td>8. Make cyber risk governance an essential part of your organization’s resilience approach</td>
<td></td>
</tr>
<tr>
<td>9. Choose one of the three effective cyber risk governance models</td>
<td></td>
</tr>
<tr>
<td>10. Transform effective cyber risk governance into an opportunity for better business</td>
<td></td>
</tr>
</tbody>
</table>

Figure 15.4.

Integrate Cyber into ERM and Other Key Risk-Management Initiatives

*Integrate Cyber-Risk Management into ERM*

Companies that have solid risk-management infrastructure in place will be much better off integrating cyber risk into their framework than those who take a haphazard approach to risk management, or worse, look the other way. Figure 15.5 is an evolutionary view of types of risk management that may or may not be in place at an organization—clearly those tending toward the right-hand side of this
evolutionary spectrum are more likely to be able to successfully address and integrate their cyber risk into their ERM portfolio.

Figure 15.5.

The challenge of cyber risk for the average business is, arguably, greater than any other risk they have faced before. Even for highly evolved companies with sophisticated ERM systems, it is a challenge. Let alone for those companies that hide their head in the sand when it comes to cyber risk, taking a “wait and see” or “it won’t happen to me” approach to cyberattacks. They must not have heard the FBI Director’s admonition several years ago that there are two kinds of companies: those that have been hacked and know it and those that have been hacked and don’t know it.

*Understand That Cyber Risk Is More Often than Not a Strategic Risk*

Not every risk is a strategic risk—many are operational, financial, technological, legal, environmental, and the like. But some risks are, whether because they directly affect the organization’s strategy or because of their high likelihood or severe impact.
Cyber risk can be a strategic risk mainly under two sets of circumstances: instantaneously, when it can seriously and deleteriously affect a business strategy or plan all of a sudden (witness the Sony Pictures Entertainment case), or over time, when a situation affecting a company’s and its stakeholders’ well-being has been brewing slowly, persistently, and eventually surfaces with high impact and strategic consequences (e.g., the Target case).

When a company has good strategic risk management and governance in place, integrating cyber risk is relatively speaking easier, compared of course to companies without such capabilities.

*Understand Cyber-Reputation Risk as It Relates to Your Company*

In 2007, the Economist Intelligence Unit published a study in which it identified reputation risk as “the risk of risks.” No one had taken a serious look at this issue in quite the same way before. Since then, reputation risk has become one of the top five to ten strategic risks that most concern boards and C-suites globally. Additional work has been done on understanding the full meaning of reputation risk—in one study, reputation risk is defined as follows:

Reputation risk is an amplifier risk that layers on or attaches to other risks—especially ESG risks—adding negative or positive implications to the materiality, duration or expansion of the other risks on the affected organization, person, product or service.

Under this definition, any risk, including cyber risk, qualifies as an underlying risk onto which reputation risk may layer and attach itself, “adding negative or positive implications to the materiality, duration or expansion...on the affected organization, person, product or service.” It depends heavily on whether the company in question has prepared properly for that specific risk.

The full implications of cyber reputation risk are only now beginning to be understood and have been underscored in several important industry surveys, including from Marsh and AIG, which underline that
“cyber-reputation risk” may be the “risk of risks” turbocharged. Here are the findings from the June 2016 AIG survey:

- More than two out of three executives and brokers believe that the reputational risk from a cyberattack is far greater to a company than the financial risk.
- More than seven in ten executives and brokers say legal compliance issues are making companies think more about cyber risks.
- The vast majority of brokers and executives believe hackers are the primary source of cyber threats, though nearly three-quarters of those surveyed also perceive human error as a significant component of cyber risk.

Know Your Cyber Stakeholders and Their Crown Jewels

Companies have stakeholders, from shareholders and employees to customers and regulators. Each stakeholder has one or more interests or “stakes” in the company. In the case of shareholders, it’s the protection and growth of their investment. In the case of employees, it’s the preservation of jobs, opportunity for growth and advancement. In the case of customers, it’s the protection of personal data and other entrusted customer “crown jewels.” In the case of governments and regulators, it’s the protection of lives and assets.

Governments, at the end of the day, are focused on the common threat: how to manage it and protect society. Companies should be focused on how to manage their own risks and threats in a manner that builds resilience, sustainability, and protection of stakeholder interests, and externally, collaborating and benchmarking within the private sector (developing good practices with other companies), and societally (learning from and contributing to applicable public/private partnerships). The extent and depth of such private and public collaboration will be determined by the company’s business, strategy, cyber-threat exposure, and the volume and sensitivity of its cyber-crown jewels.
Knowledge of your stakeholders and their crown jewels will go a very long way to understanding what your top cyber-risk priorities are.

*Create a Robust Cyber Culture*

It’s important to create an internal system of learning among employees and third parties about the cyber risks that they may be exposed to. This includes providing helplines/hotlines, unplanned trainings and communications modules that will help them learn the lessons that need to be learned and get accustomed to the type of threats and attempts that are most likely to occur in your business (phishing, social engineering, spoofing, etc.).

Integrate cyber-risk learning and teachable moments into your ethics and compliance or human resources or learning center scheduled and unscheduled trainings and take it all the way up to the boardroom on a regular and periodic basis.

Taking a page from the E&C paradigm, table 15.2 provides both an overview of the nine E&C paradigm elements and their cyber equivalent or similar program as well as several additional cyber-specific activities that a company should consider integrating into their Cyber-GRC program most specifically targeting the building of a cyber-resilient culture.

<table>
<thead>
<tr>
<th>Table 15.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robust Cyber-GRC Program and Its Comparison with E&amp;C Paradigm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E&amp;C Paradigm Element</th>
<th>Similar Elements within a Cyber-GRC Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. E&amp;C risk assessment</td>
<td>➢ Cyber-risk assessment (NIST/Other)</td>
</tr>
<tr>
<td>2. Code &amp; policies</td>
<td>➢ Integrate cyber risk as a key issue into existing code of conduct</td>
</tr>
<tr>
<td>3. Chief ethics &amp; compliance office resources</td>
<td>➢ Develop/integrate all necessary supporting policies &amp; procedures</td>
</tr>
<tr>
<td>➢ CISO/CIO/CRO cyber resources, budget</td>
<td></td>
</tr>
<tr>
<td>4. Board &amp; C-suite access</td>
<td>➢ Board &amp; C-suite access &amp; reporting lines for CIO/CISO/CRO periodically (quarterly) &amp; under crisis conditions</td>
</tr>
<tr>
<td>5. Training &amp; communications</td>
<td>➢ Integration of cyber training &amp; communications into company learning systems/HR/E&amp;C regular &amp; exceptional training</td>
</tr>
<tr>
<td>6. Internal controls alignment</td>
<td>➢ Close collaboration with audit, risk &amp; compliance to ensure all internal controls &amp; other systems are aligned, tested &amp; monitored</td>
</tr>
<tr>
<td>7. Helpline/hotline system</td>
<td>➢ Ensure that cyber issues are part of any helpline/hotline/concern line system within the company</td>
</tr>
<tr>
<td>8. Consistent discipline</td>
<td>➢ When cyber incidents occur internally—from employees or third parties—ensure coordination with HR, legal, compliance of any follow-on disciplinary or other action</td>
</tr>
<tr>
<td>9. Audit, monitor &amp; evaluate</td>
<td>➢ Ensure that there are several audit, monitoring, or evaluation initiatives customized to the company’s needs that take place periodically</td>
</tr>
</tbody>
</table>

➢

➢ Different/Additional Cyber-Code Program Elements

| 10. Engage in private/public partnerships | ➢ Engage in private/public partnership—ensure that appropriate contacts and connections are made with relevant law enforcement and regulators |
| 11. Integrate cyber into resilience system | ➢ Integrate cyber deeply into your company’s crisis, business continuity & data protection/recovery systems |
12. Cross-disciplinary &
cross-divisional
collaboration

- Have a cyber working group of necessary and desirable cross-
disciplinary and cross-divisional experts

13. Know your cyber jewels
& cyber actors

- Roadmap the company’s crown jewels & engage in cyber
actor/perpetrator analysis

14. Cyber-reputation risk &
stakeholder analysis

- Engage in cyber-stakeholder analysis—prioritize who they are and
prepare for reputation risk management

15. Integrate cyber into
third-party/supply-chain
management

- Extend cyber program to third parties and supply chain as
necessary or required by law

Conclusion: Cyber Resilience Begins at Home

Cyber resilience begins at home. If companies build it, regulators should respect it. The key is to create
cyber resilience through the deployment of an appropriate Cyber-GRC program that is customized to the
needs and profile of a company (just like in the example of the evolution of the E&C paradigm) and that
both the private and public sectors alike can recognize as such.

The development of a Cyber-GRC program paradigm doesn’t have to take as long as the development of
the E&C paradigm for several reasons. We live in a quicker time, when cyber-risk management cannot
wait and the wrong kind of regulatory or legal imposition can actually hinder rather than help.

Additionally, in the case of cyber risk (as contrasted with E&C risk issues), companies are largely not at
fault, and a good relationship between the public and private sectors on this topic is critical and benefits
all stakeholders—the company, the community, and society.

To wrap things up, figure 15.6 is a typology of Cyber-GRC resilience, a bird’s-eye view of the categories
of cyber-risk readiness that exist at companies on the basis of two critical criteria: (1) whether their
leadership (management and board) is taking a proactive and informed approach to Cyber-GRC as it relates to their specific business and sector, and (2) whether the specific organization operates in a medium/high to very high risk environment, sector, or footprint.

If we display this typology along an “evolutionary” spectrum (figure 15.7), we can see that only three out of the five categories would provide what we would call “effective” Cyber-GRC resilience. Companies that find themselves on the left side of this spectrum would do well to get their cyber act together, and
regulators and government agencies that deal with companies in the middle to right side of this spectrum should be grateful for the investment of time, resources, talent, and care that such companies are devoting to this singularly challenging risk.

![A Typology of Cyber-Risk Governance Readiness & Resilience: The Evolutionary Spectrum](image)

Figure 15.7.

Companies that are able to deploy a proactive and robust Cyber-GRC posture will in the process (a) comply with laws and regulations that exist for their sector better, (b) establish and deploy successful standards of behavior and cyber culture within their organizations, (c) protect themselves better and in a more informed way from cyber threats, (d) help to shape and influence the development of industry-wide frameworks for the tackling and handling of such new threats and challenges, and (e) maybe even find opportunity within their cyber risk to add value either through process improvements or even enhancements within their portfolio of products and services. See figure 15.8.
Endnotes

1 While this chapter focuses on corporations and business, the suggestions made throughout this chapter are organizationally applicable to any other form of entity including nonprofits, universities, and even governmental agencies, national and international.


3 The bribery scandals of the 1970s (leading up to the passage of the US Foreign Corrupt Practices Act in 1977 (FCPA); the US savings and loans scandals of the 1980s; the healthcare fraud scandals of the 1990s; Enron et al. at the turn of the century (leading up to the passage of the Sarbanes Oxley Act in 2002); the financial scandals and meltdown of 2008 (leading up to the passage of the Dodd Frank Act in 2010); etc.


5 Ibid, p. 84.

6 Though in this chapter we stress the voluntary nature of the E&C paradigm, it is important to note that when a company strays into alleged or actual illegal conduct, it is investigated and/or prosecuted by the government; if the
prosecutors find that the company did not have an effective E&C program in the first place, short of prosecution, the government may impose a monitorship (an external expert to oversee the company’s E&C and other operations, sometimes for years), a deferred prosecution agreement (DPA), and/or corporate integrity agreement (CIA) on the company, which for all intents and purposes, will require it—involuntarily—to create an effective E&C program. If it is found that, at the end of such monitorship, DPA, or CIA, the company has not complied with the creation of an effective E&C program, the prosecution may come down with its full prosecutorial force on that company and be far less compromising on any fines, settlements, or jail terms for executives. Thus the E&C paradigm, when adopted in advance of actual or alleged E&C illegal behaviors, will not only act as a risk mitigant or preventer but also provide the company with a shield and defenses (almost like an insurance policy) in the event of a violation. There is growing body of evidence that the E&C paradigm, when properly developed within a company, will be seriously taken into account by prosecutors when they investigate a company for alleged wrongdoing.

Today, several major organizations exist in the United States and Europe that are devoted to the issue of building internal organizational business conduct programs. Among them are the original associations of this kind: the Ethics Resource Center (ERC) and the Ethics & Compliance Officer Association (ECOA)—which merged in 2015 and are now known as the Ethics and Compliance Initiative (ECI); a number of other US and non-US-based organizations such as the Society for Corporate Compliance and Ethics, the Open Compliance and Ethics Group, the Institute for Global Ethics, the UK-based Institute of Business Ethics, the French- and Belgian-based Cercle D’Ethique des Affaires/Cercle European des Deontologues; and a number of national associations such as the Association of Compliance Officers of Ireland or regional associations such as the Australasian Compliance Institute and the European Business Ethics Network. None of these organizations, except for the ERC, which in turn, played a major role in the creation of the DII, existed before 1992 when the ECOA was founded. The FCPA Resource Guide of 2012 made heavy reference to the Ethics and Compliance Handbook published in 2008 by the Ethics and Compliance Office Association (now ECI) in which fifteen leading chief ethics and compliance officers deliberately developed each of the major elements of an effective E&C program on the basis of the USSG. A very recent development at the DOJ involved its fraud division hiring a member of the private sector, an ex-chief compliance officer of several leading companies, as an in-house expert to determine whether companies under investigation or prosecution had “effective E&C programs” in place, which might give them a break from prosecution or on the amount of fines or settlements that might otherwise be applicable under the law.

Chapter 8 specifically provides that organizations that are found to have committed a crime and do not have compliance and ethics program elements in place to prevent or detect such crime may not get the benefit of reductions in fines, jail terms, and other penalties. Refer to US Sentencing Guidelines Manual Section 8B2 at www.uscc.gov/2007guid/8b2_1.html.

See the original DII Principles at www.dii.org/resources/dii-charter.pdf.


Ibid.


Two out of the five proactive Cyber-GRC companies profiled in *Emerging Practices in Cyber-Risk Governance* not only had effective programs in place but also developed and deployed cyber-related products and services (cyber-risk software and cyber-risk insurance) for sale to their customers. Bonime-Blanc, *Emerging Practices in Cyber-Risk Governance*. 
The Cybersecurity Social Contract is a comprehensive assessment of the state of cybersecurity. As a blend of high level strategic advice and more focused recommendations it offers the next administration and Congress a road map for sensible and practical progress dealing with the urgent security issues we face.

— Michael Chertoff, Executive Chairman and Co-Founder, the Chertoff Group; former Secretary, US Department of Homeland Security

I have focused on the importance of cyber threats to the nation since the early 1990’s. This well researched and documented book is the most comprehensive work to date in addressing these strategically important issues. I strongly recommend the administration and the Congress adopt the recommendations of this work.

— Admiral Mike McConnell (Retired), former US Director of National Intelligence; former Director, National Security Agency

The Internet Security Alliance continues to be a pathfinder for cybersecurity. The Cybersecurity Social Contract outlines more than a dozen near term actions that the next president and Congress should undertake. It provides a thoughtful roadmap of recommendations that places risk management principles at the core of the next administration’s cybersecurity agenda.

— Melissa Hathaway, President, Hathaway Global Strategies; former Acting Senior Director for Cyberspace, National Security Council; former Director of the Joint Interagency Cyber Task Force

What an accomplishment. The Internet Security Alliance continues to prove its thought leadership by laying out a practical framework that integrates technology, government policy and business economics. The Cybersecurity Social Contract is a thoughtful guide that advances our nation’s cybersecurity.

— Air Force General Charlie Croom (Retired), Vice President, Cyber Strategy and Government Relations, Lockheed Martin; former Director, Defense Information Systems Agency

The Cybersecurity Social Contract fills a gaping hole in the cybersecurity discussion. For the first time technical expertise has been blended with the real world economics and the politics. This volume offers the incoming administration the best hope for making serious progress in addressing the growing cyber threat.

— Pradeep Khosla, Chancellor, University of California—San Diego; former Dean, College of Engineering, Carnegie Mellon University

The Cybersecurity Social Contract presents a comprehensive overview of the cybersecurity issues facing us today, why we have failed to get our arms around these issues—including privacy—and what the next administration needs to do to avoid catastrophe and create a digital world that allows all of humanity to prosper.

— Art Coviello, Jr., Executive Chairman (Retired), RSA