PROTECTING YOUR DIGITAL BUSINESS

BEYOND CYBERSECURITY

JAMES M. KAPLAN • TUCKER BAILEY • DEREK O'HALLORAN
ALAN MARCUS • CHRIS REZEK

WILEY

BEYOND CYBERSECURITY

PROTECTING YOUR DIGITAL BUSINESS

James M. Kaplan
Tucker Bailey
Chris Rezek
Derek O'Halloran
Alan Marcus

WILEY

Cover image: ©mistery/Shutterstock
Cover design: Wiley

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

ISBN 9781119026846 (Hardcover)
ISBN 9781119026914 (ePDF)
ISBN 9781119026907 (ePub)

Contents

List of Tables

List of Illustrations

Foreword

We live in a remarkable age of technology innovation. The speed with which we are able to communicate, collaborate, and transform our businesses and organizations is truly astounding. Yet the risk created by our increasing dependence on those technology advancements is equally astounding. The economic, operational, and reputational risks of technology are well known to anyone who has paid even passing attention to the almost daily security breach headlines.

In their research, so effectively laid out in this book, the authors explain why there is so much cyber insecurity today, how it has become such an intractable problem, why it could get worse, and what organizations, industries, and governments must do now to start to address the problem. Importantly, James Kaplan, Tucker Bailey, Chris Rezek, Derek O'Halloran, and Alan Marcus go beyond elucidating today's risks and how to mitigate them, and extrapolate the downstream economic consequences if organizations don't change their fundamental approach to cybersecurity.

During the course of the authors' work, I had an opportunity to preview their methodology and early results. So much of what they were seeing in organizations around the globe mirrored what I had been seeing and hearing from RSA's customers. As the authors subsequently presented their early findings to national representatives of countries from Europe, Asia, and the Americas at the 2014 RSA Conferences, it was clear that their findings resonated globally and reflected a universal experience. At these sessions, I was encouraged to see such an improved understanding of the need for all nations to cooperate to solve this problem.

It is clear from the research that the advent of cloud, mobile, and social media technologies combined with contemporary digital business practices has so expanded and distorted the attack surface of organizations that it is no longer possible to use the perimeter as an effective defense method. The perimeter that used to serve as a barrier between organizations and the external world has been perforated to the point that even a Swiss cheese metaphor is too charitable. The perimeter has become fragmented, ephemeral, dynamic, and contextual. As such, the security programs and controls on which we have relied are being overwhelmed. A new security model is called for and the authors of this book are recommending a multitiered approach based on the concept of digital resilience—an approach that has been adopted by leading companies around the world and has rapidly become conventional wisdom.

Digital resilience is not just a theory. It is a strategy, yes, but it is also a framework of policies, processes, and controls that promise real security in our increasingly insecure world. It starts with a thorough understanding of risk and the need to view digital risk through the lens of an organization's business objectives, priorities, and critical assets. It's about creating a culture of security among business leaders so that digital business decisions are made with security in mind and not just as an afterthought. It's about being prepared for attacks from any source, including insiders, and having the visibility, analytical tools, and dynamic controls necessary to respond rapidly and with agility to the inevitable intrusions. Most of all, digital resilience is about bringing all of these elements together in a coherent whole to create true defense in depth.

But our organizations are not islands. It's hard for them to succeed on their own. The authors acknowledge the need for an ecosystem of governments, regulators, vendors, and

industry groups in which organizations work together and create policy that will protect the collective whole.

For many, the topic of cybersecurity continues to be unfathomable. A lack of organizational maturity, fear, and a sense of hopelessness permeate many organizations. As the authors explain in their analysis of the economic consequences of continued cyber insecurity, the impact of this lack of clarity goes beyond the current challenges we face, since the adoption of innovative, potentially transformative technologies is being hampered by fear and uncertainty around cyber risks. But, as two-time Nobel Laureate Marie Curie said, “Nothing in life is to be feared. It is only to be understood. We must understand more so that we may fear less.”

The authors do an exceptional job of creating that understanding in this book and are to be commended for providing the research and analysis necessary to distill such a clear and compelling path to a secure future.

I believe this book can be of enormous help to security practitioners and IT executives, not only to benchmark themselves against real-world successes, but as a tool to explain to senior management the importance and relevance of cybersecurity to their organizations’ future and very viability.

Every politician and regulator should use this book as a guide for developing thoughtful, effective policy and practical regulation that can support the private sector in its efforts.

And, finally, for executives and boards of directors, it can be a valuable guide for their fiduciary understanding of a problem that all organizations face and will only grow in import in the future. I am frequently invited to speak to boards of directors about their cybersecurity situations and

outlook, and, while I frequently draw upon my own experience and the experiences of our customers around the world in those conversations, I’m thankful to be able now to share the excellent insight and perspective of this book as well.

Arthur W. Coviello, Jr.
Executive Chairman
RSA, The Security Division of EMC

Preface

Progress for the world economy depends on tens of trillions of dollars in value being created from digitization over the next decade. Institutions are moving from having pockets of automation to using pervasive connectivity, massive analytics, and low-cost scalable technology platforms to achieve fundamentally different levels of customer intimacy, operational agility, and decision-making insight. In banking, this means opening accounts and approving mortgages in minutes rather than days or weeks. In insurance, better underwriting and fairer pricing based on massive analytics. In airlines and hotels, it means more transparency and less hassle for travelers.

When “everything is digital,” private, public, and civil institutions become more dependent on information systems. In such a hyperconnected world, online and mobile capabilities increase these institutions’ vulnerability to attack by sophisticated cyber-criminals, political “hacktivists,” nation-states, and even their own employees. As a result, the success of continued digitization hinges on consumers and companies trusting that financial records, patient data, and intellectual property will remain confidential, valid, and available when required in the face of increasingly determined cyber-attacks.

Protecting institutions from cyber-attacks is therefore critical to continued economic development, which led the World Economic Forum and McKinsey to collaborate to raise the visibility of cybersecurity among C-suite executives at the Forum’s 2014 Annual Meeting in Davos.

We agreed that two outputs would be critical: a fact-based point of view on the broad strategic and economic of

implications of cyber- attacks, and a plan for what the full set of players in the cybersecurity ecosystem should do to achieve digital resilience, with a strong focus on how senior executives could address this as a business rather than a technology issue.

Based on interviews, surveys, and working sessions involving executives at several hundred institutions, our research yielded four findings.

First, without dramatic changes both in the way institutions protect themselves and in the external support they receive, the risk of cyber-attack will reduce trust and confidence in the digital economy—reducing the value created by $3 trillion in 2020. To counter this, the world's institutions will have to achieve a state of digital resilience. Only then will they be able to capture the value of a hyperconnected world despite the risk of operational disruption, intellectual property loss, public embarrassment, and fraud that cyber-attacks create.

Second, although there is a high degree of consensus on the practices required for digital resilience, companies are not putting them in place fast enough. Digital resilience requires companies to integrate cybersecurity deeply within their business processes and information technology (IT) environment. Unfortunately, to date, most companies continue to treat cybersecurity as a control function, which causes increasing friction between the need to protect their valuable information assets and digital processes on the one hand and the need to extract value from technology investments on the other. Even the largest and best-funded institutions design their cybersecurity programs backwards, starting with technology controls rather than business risks, and failing to drive the broader organizational and business process change required.

Third, in order for companies to achieve digital resilience, they will need to improve the collaboration between their cybersecurity team and the business, increase the entire IT organization's focus on resiliency, and dramatically upgrade the skills and capabilities of the cybersecurity function. Only the CEO and the rest of the senior management team can drive organizational change of this scale.

Finally, although nobody can protect companies from cyber-attacks but themselves, regulators, law enforcement, defense/security agencies, technology vendors, and industry associations will all have important roles to play in creating an ecosystem that enables digital resilience. Although there is much less consensus on how the broader digital ecosystem should evolve than on the actions individual companies should take, increased collaboration across the public, private, and not-for-profit sectors will be critical.

SETTING THE CONTEXT FOR DIGITAL RESILIENCE

Thinking about digital resilience requires an understanding of cyber-attacks and cybersecurity and how they fit into the digital ecosystem.

Cyber-attacks: Risks across the Business Model

In an increasingly digitized economy, all the world's important institutions depend on "information assets," structured and unstructured information such as customer data, intellectual property, and business plans, as well as on online processes that include everything from customer servicing to vendor payments. Cyber-attacks compromise information assets to further attackers' personal, economic,

political, or national-strategic objectives. While the popular press has focused on a few examples of cyber-attacks, typically theft of intellectual property and credit card information, companies have to take a broader range of potential risks into account (Table P.1).

TABLE P.1 Companies Face a Wide Range of Cybersecurity Risks

Type of Risk	Actor	Attack
Competitive disadvantage	Foreign competitor	Steals sensitive business plans to gain economic advantage
	Foreign intelligence agency	Steals intellectual property for reasons of national advantage
	Employee leaving for new company	Takes customer account information with her as she leaves to work for a competitor
Regulatory and legal exposure	Cyber-crime organization	Steals customer data to use later to undertake identity theft or medical fraud
Reputational damage	Employee	Releases sensitive documents to the public because he disagrees with company policies
	Hacktivist	Exfiltrates and releases confidential management discussions publicly because it disagrees with company policies
Fraud and theft	Cyber-crime organization	Corrupts an online financial transaction to undertake fraud
	Cyber-crime organization	Threatens to destroy important information assets unless it receives a ransom

Type of Risk	Actor	Attack
Business disruption	Terrorist organization	Changes data required for critical business processes to harm a country or organization it despises
	Insider	Destroys corporate data because he suspects he will be fired
	Hacktivist	Disrupts business processes (like online customer service) to draw attention to a cause

Cybersecurity: How Companies Have Protected Themselves

Cybersecurity[1] is the business function of protecting an institution from the damage caused by cyber-attacks in the face of constraints such as other business objectives, resource limitations, and compliance requirements. It has three facets: risk management, influencing, and delivery.

Cybersecurity is first and foremost a *risk management function*—there is no way to prevent all cyber-attacks from happening. As one chief information security officer (CISO) puts it, “My job isn’t to reduce risk. My job is to enable the business to take intelligent risks.”

If a company launches a new mobile servicing platform for customers, it is taking a risk—the mobile platform creates a new way for attackers to get at company data. But it is also seeking a return: it hopes the platform will improve revenues per customer. As a risk manager, the CISO helps business leaders make intelligent decisions about the risk of cyber-attack by answering questions such as:

- What are the risks associated with a new mobile platform? Does the business return justify the incremental risks?
- How can the mobile platform be designed to yield the best possible customer experience (and therefore business impact) at the lowest risk of losing data to a cyber-attack?

Cybersecurity is also an *influencing function*. The decisions CISOs make in tandem with business leaders on the right mix of risk and return lead to far-ranging actions across different parts of the organization: procurement teams have to negotiate security requirements into contracts; managers must limit the distribution of sensitive documents; developers have to design secure applications and write secure code. Cybersecurity necessarily involves a wide variety of stakeholders, some of whom need to be guided by compliance, some by less rigid and more persuasive measures.

Finally, cybersecurity is a *delivery function* that includes managing both technologies such as firewalls, intrusion detection, malware detection, and identity and access management, and also activities that are focused primarily on protecting information assets and online processes such as compiling and analyzing threat intelligence and conducting forensic analysis.

Naturally, cybersecurity as a business function is not the same as cybersecurity as an organization. A company may decide to consolidate all or most risk management, influencing, and delivery activities into a single cybersecurity group or distribute them among several organizations.

The Digital Ecosystem: Companies Cannot Protect Themselves Alone

Although institutions must protect themselves, they do so in the context of a broader digital ecosystem (Figure P.1), which includes:

- *Business customers*. Given the need to connect corporate networks to ease collaboration, business customers are a source of risk and vulnerability for many companies. Attackers may use a customer's IT environment as a way into a supplier's network. Equally, business customers worry about how their suppliers protect data. Both situations can create stringent security expectations and requirements for many companies.
- *Retail customers*. Consumers are not yet as sensitized to the risk of cyber-attacks as businesses, but their expectations about how companies should protect their data are starting to influence their buying decisions.
- *Business suppliers*. Suppliers such as law firms, accounting firms, banks, and business process outsourcing providers will handle a company's most sensitive data at some point. In addition, like business customers, suppliers can provide an entry point for attackers, given the interconnection of corporate networks.
- *Technology suppliers*. Vendors are a source of both risk and risk remediation. Any technology a company buys may have security flaws that create vulnerabilities attackers can exploit. However, technology vendors also offer products and services that enable companies to reduce risk by eliminating vulnerabilities, analyzing cyber-attacks, and otherwise protecting their corporate technology environments.

- *Government agencies*. The public sector—in the form of different types of agencies or ministries in each jurisdiction—plays multiple roles that affect the cybersecurity environment. It investigates attacks and prosecutes attackers. It regulates private companies, sometimes requiring specific protections or retaining the right to approve a company's cybersecurity strategy. It may also adjust civil law, provide subsidies, perform research, share intelligence, disseminate know-how, or provide capabilities with the objective of reducing the economic damage from cyber-attacks.
- *Civil society groups*. There is a huge range of civil society groups that participate in the digital ecosystem, from industry associations to standards-setting bodies and advocacy groups.
- *Insurers*. Cyber-insurance is in its early days, but even today carriers can enable companies to transfer some risks related to cyber-attacks in return for cash premiums.

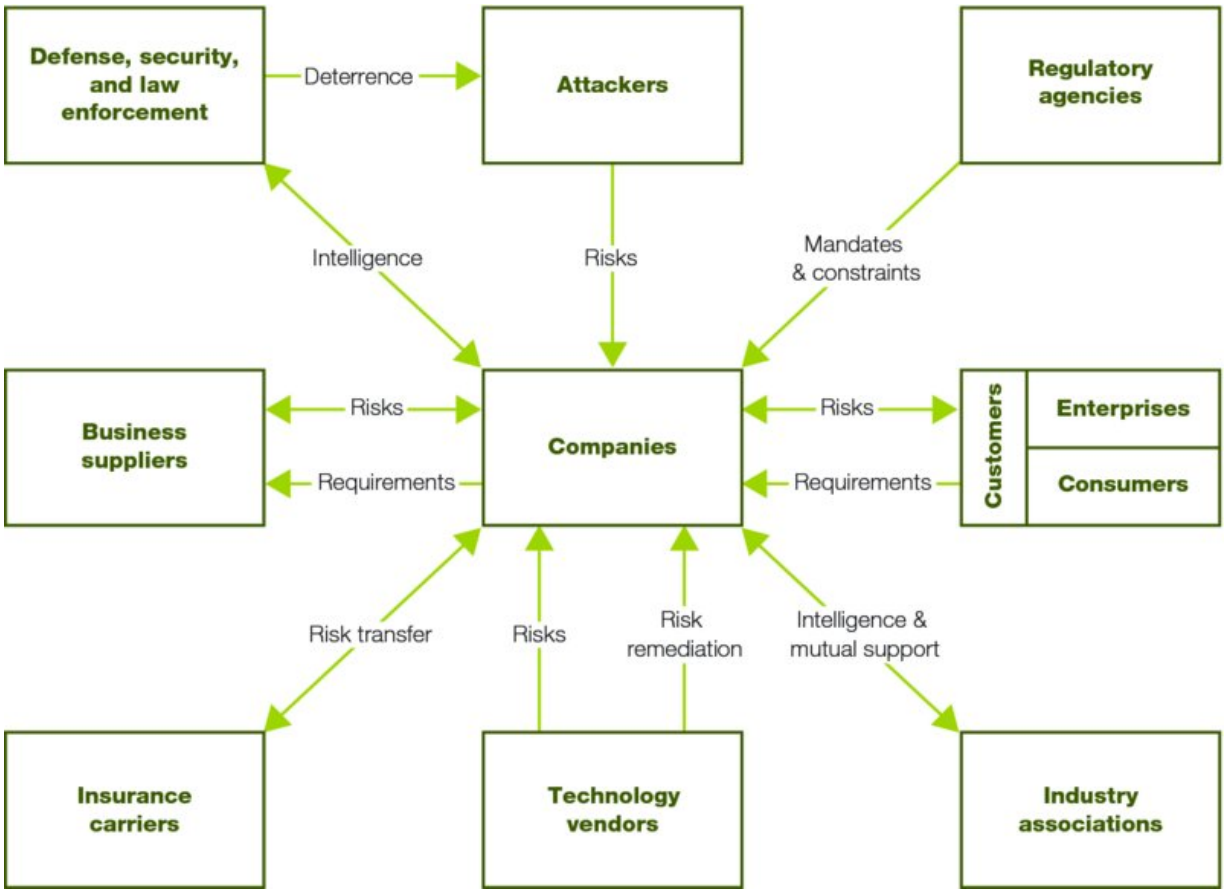

FIGURE P.1 Companies Face a Wide Range of Cybersecurity Risks

What Do We Mean by Digital Resilience?

Senior executives sometimes ask chief information officers (CIOs) and CISOs when cybersecurity will be solved—when the risk of cyber- attack will go away and they can stop worrying about it. Sometimes they draw an analogy with commercial aviation. At the dawn of the jet age, there were some horrifying crashes. Now, while airlines continue to pay obsessive attention to safety, the cab ride to the airport is typically the most dangerous part of air travel.

Indeed, driving may be a better analogy for cybersecurity. A vastly wider group of people undertakes a vastly wider set of activities using a vastly wider range of vehicles than is the case with commercial aviation. As a society, we could

choose to reduce automotive fatalities to almost zero by increasing the driving age to 30 and reducing the speed limit to 25 miles per hour, but that would have a devastating impact on the value of personal transportation.

Or take financial risk. A banking CEO would never ask when she can stop worrying about market and credit risk. She understands that her institution is in the business of accepting these risks in exchange for economic returns. Therefore, her business depends on understanding market, credit, and other risks and managing them appropriately in the context of potential returns.

Given increasing digitization, rapid technology innovation, and attackers that may be beyond the reach of law enforcement, the world economy cannot expect to eliminate the prospect of cyber-attacks anytime soon. Companies and economies can, however, aspire to achieve a state of digital resilience in which:

- Companies understand the risks of cyber-attacks and can make business decisions where the returns justify the incremental risks.
- Companies have confidence that the risks of cyber-attack are manageable, rather than strategic—they do not put the company's competitive position or very existence at risk.
- Consumers and business have confidence in the online economy—the risks to information assets and of online fraud are not a brake to the growth of digital commerce.
- The risk of cyber-attack does not prevent companies from continuing to take advantage of technology innovation.

It is in this context that the World Economic Forum and McKinsey & Company have collaborated to understand how

to help both companies and countries reach their aspirations.

BACKGROUND AND APPROACH

“Risk and Responsibility in a Hyperconnected World” has been a theme for the World Economic Forum since 2011. Since the middle of 2012, the Forum has worked with nearly 100 companies to sign the “Principles for Cyber-Resilience.” Adhering to these principles commits companies to recognize that all parties have a role in fostering a resilient digital economy and to develop a practical and effective implementation program. It also encourages executive-level awareness and leadership of cyber-risk management and, where appropriate, it encourages suppliers and customers to develop a similar level of awareness and commitment.[2]

For the Forum’s 2014 meeting in Davos, it asked McKinsey to help it increase C-suite executives’ level of engagement with cyber-attacks, cybersecurity, and digital resilience across industries, including not only technology and telecommunications, but also financial services, manufacturing, consumer goods, transportation, energy, and the public sector.

Jointly, McKinsey and the Forum decided that the most useful outputs of this project would be a fact-based point of view on the broad strategic and economic implications of cyber-attacks; and a plan for what the full set of players in the cybersecurity ecosystem should do to achieve digital resilience, with a strong focus on how senior executives could address this as a business rather than a technology issue.

We began collecting data in the late spring of 2013, developed and validated our hypotheses through the

summer and fall, and shared our findings at the Forum's Annual Meeting in Davos in January 2014.

The Fact Base

Interviews with more than 180 CIOs, CISOs, chief technology officers (CTOs), chief risk officers (CROs), business unit executives, regulators, investors, policymakers, and technology vendors provided input into how all the different participants in the ecosystem thought about the overall cybersecurity environment. In addition, surveys of nearly 100 enterprise technology users gave us a clear understanding of business risks, the threat environment, and the potential impact of a range of actions. Finally, more than 60 Global 500 institutions participated in a detailed survey on their cybersecurity risk management practices (Table P.2).

TABLE P.2 Our Research Was Based on Extensive Surveys and Workshops

Sources of Input	
Interviews with 180+ industry leaders	CIOs, CISOs, CTOs, CROs, and business unit executives in financial services, insurance, health care, high-tech/telecom, media, industrial, and public sectors Policymakers, regulators, and members of the defense and intelligence communities Across the Americas; Europe, Middle East, and Africa (EMEA); and Asia
Survey of nearly 100 technology executives	Covered: • Most important business risks • Business implications of risk of cyber-attacks • Perspectives on external environment • Actions for improving resilience
Cyber-Risk Maturity Survey results from 60+ companies	Assessment of cybersecurity risk management capabilities based on 180 best practices Included financial services, health care, insurance, and other participants from the Americas, EMEA, and Asia

Sources of Input	
Validation in range of forums	Tested at events involving more than 500 executives, policymakers, academics, and other thought leaders: • World Economic Forum events in Geneva; Washington, D.C.; New York; Davos; Baku; Brussels; and Dalian, China • McKinsey convened forums for CISOs in the banking and health care industries

Scenarios and Economic Impact

Based on insights gleaned in the interviews, we identified more than 20 drivers of how the cybersecurity environment could evolve over the next five to seven years and synthesized those into two macro-level drivers: intensity of threat and quality of response. From there, we derived three future state scenarios: muddling into the future, digital backlash, and digital resilience. Based on input from the interviews and surveys, we estimated how each scenario would affect the adoption of a range of important technology innovations such as cloud computing, enterprise mobility, and the Internet of Things—and what impact this would have on value creation.

Critical Actions to Achieve Digital Resilience

Again, based on the interviews and surveys, we highlighted the most important actions for each participant in the cybersecurity ecosystem, with a particular focus on the actions individual companies would have to take across all their business functions to protect themselves.