# 1.0

# INTRODUCTION



*There are two kinds of companies. Those that have been hacked, and those that have been hacked but don't know it yet.*[1]
House Intelligence Committee Chairman Mike Rogers

## 1.1 DEFINING CYBERSECURITY

When Congressman Mike Rogers included the words above in a press release to announce new legislation designed to help better defend American business against cyber threats, many executives were alarmed over the prospect that their businesses likely were already victims of hackers. They were shocked.

We weren't.

For over 30 years, we have been deeply involved in not only building, integrating, and defending complex information technology (IT) systems but also in running and managing businesses that have come to rely on IT to create value and deliver profits.

[1] Mike Rogers and Dutch Ruppersberger, "Rogers & Ruppersberger Introduce Cybersecurity Bill to Protect American Businesses from "Economic Predators," November 30, 2011, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/113011CyberSecurityLegislation.pdf. Accessed on December 13, 2013.

*Cybersecurity for Executives: A Practical Guide*, First Edition. Gregory J. Touhill and C. Joseph Touhill.

During our professional careers, we have seen IT systems grow from stand-alone computers to today's globally connected information ecosystem that permits users to access information anytime, anywhere. We also have seen the increase in the numbers of hackers and others who attempt to gain access to information for reasons that include curiosity, personal profit, or competitive advantage. Threats to your vital information are real and intensifying.

While the term "cybersecurity" is creeping into discussions in boardrooms around the world, we find that most executives, while certainly cognizant of the importance of IT to their businesses, need help to understand what cybersecurity is, how to integrate it into their businesses to provide best value, and how to invest wisely to protect their vital information.

Cybersecurity is a relatively new discipline. It is so new that there is no agreed-upon spelling of the term nor is there a broadly accepted definition. Many people believe cybersecurity is something you can buy in increments, much like a commodity. Others believe cybersecurity just refers to technical measures, such as using password protection or installing a firewall to protect a network. Still, others believe it is an administrative and technical program solely in the realm of IT professionals. Some think it refers only to protection against hackers. We view it differently and define it as follows:

> Cybersecurity is the deliberate synergy of technologies, processes, and practices to protect information and the networks, computer systems and appliances, and programs used to collect, process, store, and transport that information from attack, damage, and unauthorized access.

We view cybersecurity as a holistic set of activities that are focused on protecting an organization's vital information. Cybersecurity includes the technologies employed to protect information. It includes the processes used to create, manage, share, and store information. It includes the practices such as workforce training and testing to ensure information is properly protected and managed. Effective cybersecurity preserves the confidentiality, integrity, and availability of information, protecting it from attack by bad actors, damage of any kind, and unauthorized access by those who do not have a "need to know." *In today's business environment, cybersecurity is not just a technical issue, it is a business imperative*.

## 1.2 CYBERSECURITY IS A BUSINESS IMPERATIVE

Executives across every business sector are increasingly concerned about cybersecurity. After all, reports indicate hacking incidents are on the rise with an estimated nearly one billion hacking attempts in the final quarter of 2012 alone.[2] New governmental laws and regulations place a premium on cybersecurity controls. Lawsuits lodged in the wake of cybersecurity breaches continue to mount in volume and damages. Customers,

[2] Nick Summers, "Hacking Attempts will Pass One Billion in Q4 2012, Claims Information Assurance Firm," November 12, 2012, http://thenextweb.com/insider/2012/11/12/hacking-attempts-to-pass-one-billion-in-final-quarter-of-2012-claims-information-assurance-firm/#!pQLJh. Accessed on December 13, 2013

shareholders, and potential investors increasingly are demanding that effective controls are put in place to protect sensitive information and avoid liabilities. Clients expect that their personal and financial information will be protected from unauthorized disclosure and possible exploitation. Executives recognize that their vital corporate information, such as their intellectual property and trade secrets, provides a powerful competitive advantage for their businesses and needs to be protected. They want to invest wisely in cybersecurity, but don't want to break the bank. Many don't know how their investments in cybersecurity draw positive returns. Additionally, because many cybersecurity measures rely on complex technical controls, many feel uncomfortable with the terminology of the information technologists, many of whom often focus more on the technology than the business it supports. The resulting language gaps create barriers that sometimes produce organizational friction, lack of communication, and poor decision-making. Discussions with our clients convince us there is an acute and growing need to help executives understand and cope with the problems posed by cybersecurity issues.

George Polya, a famous twentieth-century mathematician, said the first step in solving a problem is to understand it.[3] We agree and wrote this book in the hope that it would help executives from all business sectors better understand the nature and extent of cybersecurity and learn how to train personnel to combat cyber attacks, how to recover from such attacks, how to prevent infections, and how to best manage their business to incorporate best practices in cybersecurity.

We propose that the best way to address cybersecurity is to do so from the perspective of a manager rather than a technologist. Cybersecurity is not solely a technical issue. It affects every business function. Every activity in virtually every business relies on information to maintain a competitive advantage. Managers at every level need to understand how investing in cybersecurity produces effective, efficient, and secure results. That, in turn, produces value.

As senior executives ourselves, we recognize that a discussion of cybersecurity with fellow executives should not be too "technical," because such discussions could diminish this book's utility.[4] Executives run the entire organization, and they don't need to be focused on the coding techniques of their computer programmers. Rather, their job is to optimize the human and physical resources and assets of the organization in order to fulfill its mission safely, profitably, and beneficially. We understand that a prime focus of executives is risk management, and that is where discussions of cybersecurity should begin.

*Cybersecurity is about risk management*. It is about protecting your business, your shareholders' investments, and yourself while maintaining competitive advantage and protecting assets. It is not just about IT. Rather, it is a multidisciplinary approach to managing risk, a principal concern of every executive. Note that in addition to Chapter 3.0's emphasis on risk management, discussions of risk and risk management are prominently interspersed throughout this book.

[3] George Polya, *How to Solve it, A New Aspect of Mathematical Method*, Princeton University Press. Princeton, NJ, 1945, p. 6.

[4] Some people may refer to that meaning "don't make it too geeky," while others may say that the focus should be on the ends (i.e., the effects) rather than the means (i.e., the technology). In this case, we believe both are apropos.

## 1.3 CYBERSECURITY IS AN EXECUTIVE-LEVEL CONCERN

In our professional dealings, we have had interactions regarding cybersecurity with numerous senior executives and board members. All are highly intelligent and exceptionally talented individuals who understand their businesses inside and out. Nonetheless, many express great frustration in understanding cybersecurity and integrating it into their management processes. Here are some noteworthy concerns from some of our clients:

> I have several people who do cybersecurity for us, but we don't speak the same language. I don't understand what they say and I'm not sure they understand me either. I guess we just have to trust each other.
>
> I know that cybersecurity is important, but I don't know how well we are doing. How do I measure it?
>
> Sure, we have a cybersecurity program. How good is it? Okay, I think.
>
> I am concerned because I don't know whether I am spending too much, too little, or just the right amount on cybersecurity. I don't like playing Goldilocks.
>
> I am not sure what questions about cybersecurity I should be asking.

Some of these concerns might sound familiar to you. Perhaps you share some of these same concerns. If you do, you are not alone. According to IBM, who manages IT services for customers around the world, their clients average 1400 cyber-based attacks per week.[5] Malicious activity continues to increase from what are commonly called "bad actors," those who attempt to collect, disrupt, deny, degrade, or destroy information or the systems that collect, process, store, transport, and secure that information. Executives at all levels and in all business sectors need to be on heightened alert to threats, understand their vulnerabilities, and take appropriate action to protect their information. Cybersecurity has emerged as a leading concern of executives around the world, and it appears it will remain so for the foreseeable future.

## 1.4 QUESTIONS TO ASK

Have you ever noticed that great executives often seem to know the right questions to ask? Peter Drucker said, "The leader of the future will be a person who knows how to ask."[6] We submit that such a future is upon us right now. In today's business environment, asking the right questions is indispensible for executives at all levels. According to Gary Cohen, leaders can't know everything, especially today. With information accumulating at such a rapid pace and with so many ways to access information, our coworkers routinely know

[5] IBM Global Technology Services, *IBM Security Services Cyber Security Intelligence Index*, July 2013, p. 3.

[6] Peter Drucker, The Drucker Institute at Claremont Graduate University, April 22, 2011, http://thedx.drucker-institute.com/2011/04/the-fab-five/. Accessed on December 13, 2013.

more about their work than their executives do.[7] Therefore, wise executives routinely ask a lot of questions about cybersecurity as part of their management rhythm.

Asking the right question, often to several different people, helps identify vulnerabilities, exposes defects, discovers potential areas of improvement, and illuminates budding talent that should be nurtured. Not only will asking the right questions make you appear smarter, but also listening closely to the answers will make you smarter and better prepare you to ask even smarter questions the next time.

Like our client who said, "I am not sure what questions about cybersecurity I should be asking," many of our clients ask us to help them identify the questions that they should be asking their technical staff, fellow executives, finance staff, legal counsel, and other advisors. Every business is different, and in our consulting efforts, we typically prepare specific sets of targeted questions for each client. Nevertheless, you may find the following sample generic questions helpful as you keep cybersecurity on your agenda:

- Is my computer system infected?
- How did you find out it was infected?
- If it is infected, what do I do about it?
- How did the infection happen?
- If it is not infected, what did I do right, and how can I keep it up?
- If it is infected and we have an IT system administrator, isn't he supposed to keep that from happening?
- If the system administrator isn't enough to keep me safe, who else and what else do I need?
- Do I need outside help?
- How much is this going to cost to permit us to stay safe?
- What is the extent of possible damage in dollars and cents and to our reputation?
- If I am shut down, what happens?
- What do I tell the board of directors?
- Are regular audits by insiders and outsiders a good idea?
- How does one go about these audits?
- How much will the audits cost?
- What is the cost–benefit ratio for audits?
- How do I keep my people from making dumb decisions and doing stupid things that allow "bad guys" into our systems?
- What is the best way to train my people to be safe?
- When I started in business, I remember "safety first" signs and the positive impact they had. Can I do the same thing with computers?
- If I train my employees how to protect their home computers, will it raise their awareness at work?

[7] Gary B. Cohen, *Just Ask Leadership: Why Great Managers Always Ask the Right Questions*, McGraw-Hill. New York, NY, 2009, p. 1.

- Is there any especially high-rated protection software that I should be using?
- What kind of vulnerabilities do we have?
- How often do you check for vulnerabilities?
- Is all our software up to date with the latest version and patches?
- How do I develop an overall cybersecurity strategy?
- Is there any way to be 100% safe?
- If I can't be 100% safe, how do I mitigate risk?
- To what extent is redundancy a help?
- Is our information backed up? How often? Where are back-ups stored?
- To what extent do multiple locations help?
- In the event of a major disaster to my system, how do I recover?
- Do we have a disaster recovery and business continuity plan? When was the last time it was tested? What was the result?
- Do I have internal spies and saboteurs?
- If there are internal spies and saboteurs, how do I know who they are and how do I catch them?
- What are my liabilities if my hidden viruses infect somebody else?
- Are there any public relations (PR) firms who can help me handle cybersecurity problems?
- How about having my own hackers?
- How much should I pay my computer "geeks"?[8]
- How should I hire, train, and vet my cybersecurity staff and the people who use my computer systems?
- How do I keep track of what my cybersecurity crew and the people who use my computer systems are doing?
- Are my other machines at risk? How about my pumps, chemical dosing equipment, product quality control instrumentation, and all processing systems? What about my distribution and logistics plans? Are they at risk?
- How do I protect the organization across multiple devices, that is, mobile phones and tablets?
- Who do I call for help?

We recognize that we just presented you with a lot questions. As you read through subsequent chapters of this book, you'll see that we address the issues behind these questions in greater detail and present information that likely will inspire you to ask other questions as you make cybersecurity part of your corporate culture. One of the key objectives in our book is to attempt to answer as many of the questions listed earlier as we possibly can. Upon reviewing our manuscript, we believe that we did a pretty good job in doing so. We hope you agree.

[8] Some may view use of the term "geek" to be a pejorative term; however, many IT professionals freely use the term to denote that they have achieved a high level of technical competence. In this question, our intent is to convey the latter meaning.

## 1.5 VIEWS OF OTHERS

We are not the only ones who have thought about key questions regarding cybersecurity. The U.S. Department of Homeland Security (DHS) is doing some exceptional work in the cybersecurity realm and created a list of cybersecurity questions for CEOs that we find to be very helpful. To avoid duplication, we deliberately didn't include the DHS questions in our aforementioned list; however, we believe that they are highly pertinent and are listed below. Here are the U.S. DHS's cybersecurity questions for CEOs[9].

**Five questions CEOs should ask about cyber risks**

1. How is our executive leadership informed about the current level and business impact of cyber risks to our company?
2. What is the current level and business impact of cyber risks to our company? What is our plan to address identified risks?
3. How does our cybersecurity program apply industry standards and best practices?
4. How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying our executive leadership?
5. How comprehensive is our cyber incident response plan? How often is it tested?

## 1.6 CYBERSECURITY IS A FULL-TIME ACTIVITY

You can't let your cybersecurity guard down when you leave the office. Today's executives seemingly are always connected to the Internet in one way or another. When they aren't connected, many of them don't view it as a respite; they view it as a calamity. While in their office, they rely upon a host of IT to conduct their daily business. Mobile devices such as smart telephones, tablet computers, and other such devices have untethered executives, permitting them to access information while commuting, traveling on business, or even while they are on vacation.[10] While many executives complain about being slaves to their emails and other electronic exchanges, nonetheless, they insist upon having the capability to be continually accessible.

Such accessibility requirements create interesting cybersecurity challenges. Many executives and those who work for them frequently perform work on their personal computing devices. The resulting exchange of information between home and work IT devices exposes both to potential cybersecurity threats and creates its own class of vulnerabilities. As such, we propose that *executives should treat home computing systems with the same due care and due diligence as they would their computing systems at the office*. During the course of this book, we will share tactics, techniques, and procedures that will be helpful both at home and in the office as you protect your vital information.

[9] U.S. Department of Homeland Security Publication, https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf.

[10] We recommend you avoid doing work on vacation. Nevertheless, the reality of today is that in your executive role that you need to maintain connectivity to perform your duties effectively.

Throughout this book, we emphasize that cybersecurity is about risk management and executives are in the risk management business. By making cybersecurity part of your corporate strategy and culture; by implementing comprehensive plans, policies, and procedures; and by instituting the positive management practices outlined in this book, we believe you will be best postured to manage risk, protect yourself and your business, and deliver to your customers, clients, and constituents results that are effective, efficient, and secure.