Powerpoint presentation that you must drag the business through. Consider using the framework of the business's strategy document or a pictorial representation of it, as well as a clear and concise balanced options scorecard based on your assessment and plan, along with your suggestions on risk remediations, timing, and potential costs.

7. *Meet with Business Leaders*: Finally, the business will not know this work by osmosis, and you should not wait until they ask you to discuss it after they have made certain decisions. Be proactive in meeting with executive management to discuss the current business strategy and the work you have done to ensure they are successful, and stress the importance that there are measured approaches to reduce any potential security, risk, or privacy issue that they may be concerned about. Letting them know ahead of time that "you've got this" and showing them your approach will give them confidence in driving the business forward.

The art to this approach is doing it as a normal part of your everyday operations and getting answers ahead of your internal clients concerns. Imagine how you would look if you went into a meeting about future strategies prepared to discuss potential security issues, existing risk reduction plans, the potential financial impacts or necessities pre-calculated as the executive management team is making its decision. That type of forward-looking capability helps your business make faster decisions and execute them more quickly, thus supporting opportunity costs and time-to-market considerations. That is the level of business acumen necessary to be considered a next-generation security leader.

THE CSO AND THEIR ROLE

There is no doubt that the CSO role has significantly developed and expanded in the past decade. From technology, to convergence, to legal considerations, the security executive requires broad, career-focused technical acumen across a large set of service areas while still serving as a business executive supporting the organization's goals and strategies and managing his or her business of security.

No matter how the position of the CSO develops, there are some basic fundamental concepts and requirements of which each senior security executive should be aware. This section of the chapter touches on some of these critical concepts to create a baseline expectation to be used when thinking about how you lead, how you manage, and how you drive your own organization. These expectations are not just assumed practitioner requirements; they are the expectations of your business in how you carry out and assume these responsibilities, which determine the success you have within your position.

To Protect

In a search of any generic explanation about "security" or a similar service, the word "protect" most often is associated—and for good reason. I often respond

to messages of thanks with a simple phrase: to protect and serve. Although a bit tongue-in-cheek, there's a lot of reality to that statement. As a chief security executive, your primary duty is to protect. Certainly, one can argue that your job has many more functions—as it most certainly does—and will continue to grow in the future. But that word "protect," that duty of care, the fundamental necessity to protect from harm, is by definition the primary goal of your position. Prevention of negative impact events against people, businesses, economies, technologies, and markets is why our jobs were created.

When establishing some ground rules about how we protect, security practitioners can take their cue from ancient Greek science that is still in use today by doctors who take the Hippocratic Oath. The Latin phrase primum non nocere has been a consistent part of that oath for centuries, and loosely translated it means "do no harm." There is a lot of wisdom in that statement, and for years it has been studied as a part of governmental rule, societal management, and the advancement of human studies. For our purposes, this principle of do no harm should serve as that voice in your head on a daily basis that guides you in delivering your services to the business every day. It has been the downfall of many great practitioners when they become so focused on accomplishing the mission, destroying the bad guy, driving absolute defense; they forget that their principal actions should be to enable the organization, not to reduce, restrict, or inappropriately constrain it in any way. So, to start off this conversation on how to protect, this is a reminder to be diligent and ensure you don't cause more harm by overprotecting.

Before you get all charged up and start running out to protect, you need to think about what you are protecting. When I asked some new CSOs what they thought they were protecting, I was surprised by the wide variety of answers I got but was encouraged by not only the inward look but the outward look of what they understood was at stake if they did not do their job. Broadly stated, in most cases, CSOs are focused on protecting people, assets, infrastructure, and technology. Of course, there are wide definitions associated with these. Take assets, for example. An asset can be a digital asset, such as intellectual property, or a financial instrument, such as a currency or trading document. An asset can be a building, a campus, or a supertanker. Your job is to understand which assets need protecting and exactly how to protect them.

In each of these areas—people, assets, infrastructure, and technology—the key in knowing how to protect each one is understanding the downstream residual impact of not protecting it. In one of my previous commercial jobs I worked for an electronic manufacturing company that provided storage technology for just about every Fortune 500 and government agency in the United States. At times, my decisions were not predicated on the immediateness of what would happen to the company I served, but rather what would happen if I did not successfully protect the issue, and I allowed a situation to occur that could have developed into a negative impact event affecting the technology and the structure of all of those companies and government agencies. What would that impact be? How would that affect the economies and societies we supported? These types of questions often help drive a clearer definition beyond the "what

is the risk to my business?" concern and support the creation of priorities based on the downstream residual impact of your business threats.

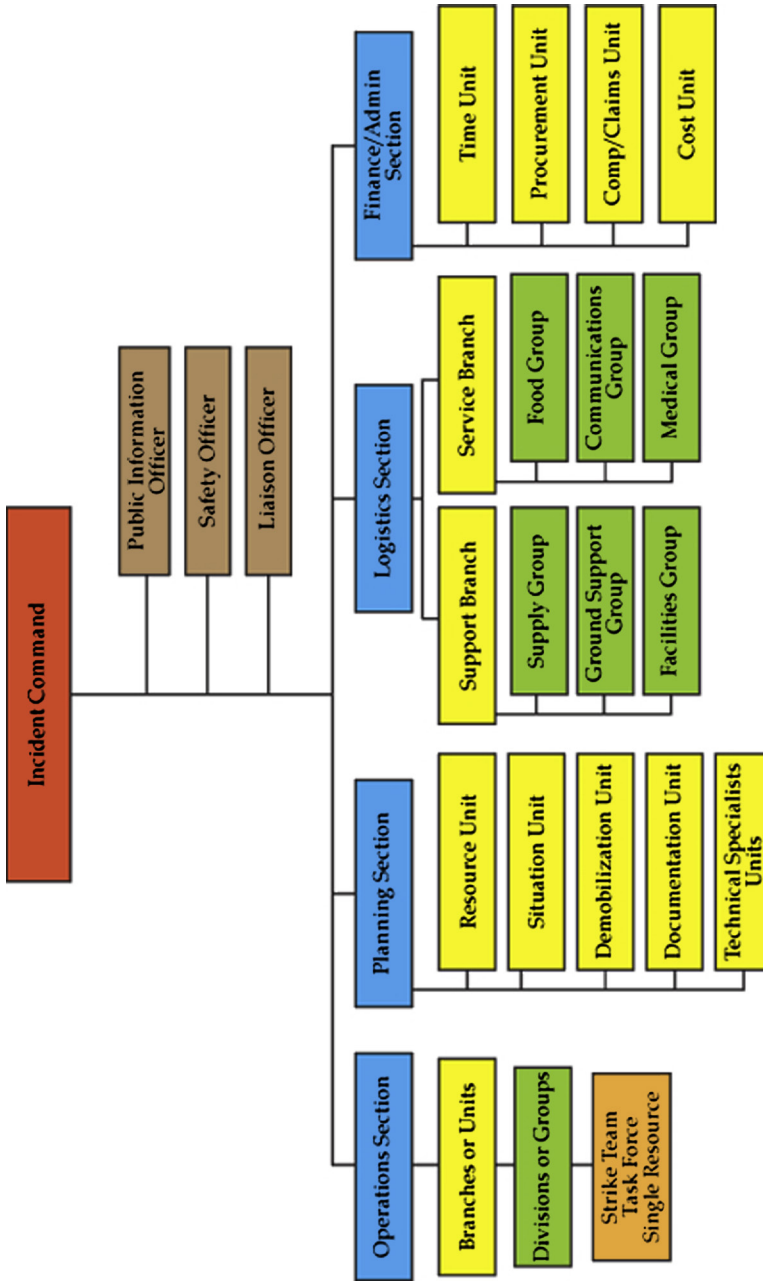
In the end, you will find that you have many things to protect. Your programs will all line to the eventual strategy of defensive operations for the prevention of harm to your business or agency. It is up to you to create that broad picture, that canvas by which your own teams will operate. By understanding your business, the environment in which you operate, and the threats associated with it, and by prioritizing your efforts to address the most critical issues facing your business, whether external or internal, you will be well positioned to protect now and in the future.

To Respond

Preventing things before they happen is, of course, the desired outcome of anyone in our business. Bad things do happen, however, and as your company's senior-most security expert, you will be seen as the chief responder, the bad things know-it-all, and you will be held accountable for preparing your company, your organization, and yourself to lead through a crisis.

In the pure sense of the word, not everything you will respond to will be a crisis. In the eyes of those you serve, however, every issue will be a crisis. Taking away labels, frameworks, and everything else associated with business resiliency and crisis response, the point here is that you need to be (and will be expected to be) the rock of any type of crisis at your business. During critical times, businesses need an authoritative anchor to help sort out the process of responding, remediating, and moving forward. Critical incidents are so broad that when one is not strictly business-related (e.g., a product failure, a brand issue, a client support issue) the business turns toward the leader who should be most capable to manage them through the crisis. That would be you.

Don't mistake knowing how to manage a crisis with knowing how to fix everything or know everything about everything. The secret of crisis management is knowing the practitionership of crisis handling. It can be argued that the same crisis response protocol can be used just as easily for a fire in one of your buildings as for a data center outage at a third-party vendor site affecting your go to market. In fact, the most mature crisis management programs incorporated in governments follow the same standards and protocol developments formulated from a program originally designed for forest fires, now referred to as the National Incident Management System (NIMS). The figure below is an example of the NIMS crisis management architecture and associated functions. Notice that the descriptions are fairly general, and all serve specific functions. Your job is not to manage all those functions, but rather to ensure leadership is assigned and trained in each of those areas. Consider becoming certified in a national or global standard of crisis management. This way, when bad things do happen, and when the business does call, you will be prepared to execute appropriately.


Incident Command
Public Information Officer
Safety Officer
Liaison Officer
Operations Section
Branches or Units
Divisions or Groups
Strike Team
Task Force
Single Resource
Planning Section
Resource Unit
Situation Unit
Demobilization Unit
Documentation Unit
Technical Specialists Units
Logistics Section
Support Branch
Supply Group
Ground Support Group
Facilities Group
Service Branch
Food Group
Communications Group
Medical Group
Finance/Admin Section
Time Unit
Procurement Unit
Comp/Claims Unit
Cost Unit

Inevitably, to call in a crisis, you need a 911 operator; rest assured that is you as well. Part of your crisis preparation must be understanding how to qualify issues, route issues, and escalate them as needed. The business needs you to help it solve and manage these issues, and you must be prepared to support it by doing this. Being prepared ahead of time by setting up simple processes and infrastructure to support this "911 function" puts you well on your way in meeting the business's expectations. There are three basic things to consider when preparing to be that 911 operator:

1. *Methods to Report*: The most important thing that you must be able to provide to your business is a capability to get information to you. Whether it's a centralized telephone number, a messaging service, an email address, a web portal site, or smoke signals, ensure you create a sustainable capability, inform the business of it, and train your people on how to operate it. Depending on the type and size your business, there may be multiple avenues of reporting critical incidents and issues, from automated alert notifications, to more basic technologies. By understanding your business, who needs to report, the best way for them to report, and even regional considerations, you will be better prepared to design systems, mechanisms, and processes to get information when its most critically needed.
2. *Notification and Escalation Mechanisms*: Once an emergent issue has been reported, your processes must require that you have a capability to get the word out as part of your incident and crisis managing capabilities. There is an infrastructure part to this, and there's a process development aspect. The process development requirement is understanding to whom and when to escalate. For different incidents and crisis types, different people have to be notified. In diversified businesses this often means that each one of your business units have their own requirements as well. Sometimes it's the entire company; in other types of emergencies in a single building, and during certain events may be your only way of notifying the crisis team of an escalation—that is the what. The how is a little different. Once you make certain decisions and have preplanned escalation and notification sequencing, you need a mechanism to deliver those messages. Again, these can be as simple as emails or manual telephone calls or as complex and integrated as automated messaging systems for SMS, phone, or web-based technologies.
3. *Issue Classification and Handling Index:* The last area of basic preparation for getting that "911 call" is to be prepared with a simple handling index for different types of issues. Applications and technologies that automate this for you are certainly available, but you can start simply by listing all the possible, potential, and probable types of incidents you may face based on the type of company or agency you are, prioritizing them by probability and severity, and populating them with data such as who is responsible for managing that type of incident, who needs to be notified, and other routing, notification, and escalation information. Of courses, this gets more complex as you take on the responsibility for more sites, more business units, and

more geographies, but the premise is the same. Know who will be calling, what they could potentially be calling about, and whom you have to call to get the ball rolling.

The Business Principals

The next critical attribute for the next-generation security leader is business acumen. As a business operations protection executive, you are required to understand how your business works and how it makes money, and be able to articulate how you support that business and enable it to meet its goals.

A crucial part of business knowledge is understanding profit. Another chapter discusses the general details of financial acumen, but the business principles of how profit is derived from the goods, services, or efforts of your organization are the underpinning connectors between all decisions made at your company. Is your business a revenue-focused company or a margin-focused company? If you are a margin-based company, what critical elements drive margin expansion? How is top-line revenue recognized at your company? What are the most critical times of the year around revenue development? These type of questions are minimum barriers to entry if you are truly a business operations protection executive. You cannot possibly begin to assess risk, prioritize threats, and direct your teams to protect the business if you are not even sure of how they fiscally operate.

Another aspect of basic business principles required for the next-generation security executive is to understand the concept of risk versus reward. I've mentioned it before and I will mention it again in this book: Your job as a CSO is predominantly risk management. How you identify, measure, and support the business in remediating, transferring, and accepting risk must be based on the profitability and financial implications of the business. This is not to say that risk shouldn't be addressed because it's too expensive; rather, we look at risks, their downstream impacts, probability factors, and many other measurements to create a financial risk picture. It is that financial risk picture that supports the decision-making process in context with the holistic operations and profitability of your company. Further, risk needs to be measured and evaluated across all other operations and profitability components of your company, such as research and development investments, service enhancements, workplace enhancements, and expense management initiatives. Sometimes this means that a risk that seems to be very straightforward and have an obvious resolution may not meet that risk-versus-reward threshold needed to move it forward, and you need to accept this. Security risk and privacy issues, although important, are only a component of your business's operations, and in most cases they are only a minor component in the context of the entire business go to market. Understanding all aspects and priorities of your organization will help you better provide to your leadership the information and data needed in making those risk decisions.

The final component of basic business principles for security executives is the concept that their job is actually to protect the business and not just provide

security. Business executives have long lamented that the "security guy" just doesn't get it, that we are paid paranoids that are incapable of putting security issues in the context of the business they are responsible for every day. Don't be that "security guy". By converting your concept of information security, corporate security, risk operations, and the like to business operations protection programs, and by starting to use the language of your business, you will be well on the way to changing the hearts and minds of those in the business. Of course, actions speak louder than words, as discussed throughout this book, and you need to implement business-focused programs that look at the entire business process, to prioritize threat management based on business needs and criticality, and to immerse yourself into operating business units to learn how they operate and to be able to articulate the services you deliver in alignment with what they deliver every day.

Technical versus Nontechnical

There is a continuing great debate at senior levels within companies when it comes to the hiring of CSOs. This debate is focused around whether the candidates should be technical. Technical acumen can be interpreted in many different ways. Technical skills for a nurse are very different than technical skills for a computer programmer and even different still for a carpenter. For the context of this book, let's assume that the next-generation security executive has converge responsibilities and the technical skills we are talking about are relative to computer, network, infrastructure, application, and business technology.

In recent years I have seen a mass migration by non–technically competent executives into the ranks of senior security leaders. In almost every case there were very different reasons why they were put into those positions. In some cases it was because of what we just discussed, specific to an inability of the incumbent to support the business in the context of the business. In others the entity was looking for financial sanity and management in what seemed like a continuously growing monster of security necessities with limited executive financial acumen within that group. For yet another, the leadership wanted someone who truly understood their business and needed new opportunity to grow in a diversified area. Of course there are hundreds more reasons why a nontechnical leader was put into the position—many good reasons that produced great results.

As the criticality around security, risk, and privacy functions in an organization continue to increase, however, and the complexities of the integration of technology into business functions increase, we need to have reasonable discussion of how technical a security executive needs to be. Let's look at it from this perspective: If you are the chief of staff for surgical operations at a hospital, should you have medical technical acumen? Most would agree that the executive leading other surgeons and managing surgical functions should have a high degree of medical knowledge. If you are the chief financial officer of a public corporation, should you not have financial technical acumen in order to deliver on the corporate responsibilities around financial management and assurance?

I strongly believe that the same level of care and consideration should go into the development of the leadership position and the expectations for an executive accountable to lead cyber defense organizations as part of an overall business operations protection program. This does not mean that they need the capability to program applications, create Python scripts, or manage deep packet inspection devices or firewalls. What it does mean is that they have a firm grasp of the technology areas that they are responsible for through education, on-the-job training, or life experience.

How much technical knowledge does the CSO need? There is no perfect measurement, guideline, or algorithm to provide an exact answer to this. The key is that they possess the right amount of knowledge to be able to effectively discharge their duties, create and execute strategy, and provide operational leadership to their organization. Understanding the basics of networking, systems management, application architecture, information and system security, cloud computing, environmental security, defense in depth methodologies, and principles of authentication, authorization, accounting, certification and accreditation, risk management, and advanced threat management are a great start. At a high level, these skill sets enable an understanding of the large majority of business technology defense architectures, allow the right level of conversation with technical resources, and enable the translation of complex security issues in a more simplistic fashion because of an understanding of the issue and an ability to translate accordingly. If you are in a technology company, your level of technical acumen needs to be significantly higher than that of an executive in a steel manufacturing firm. If you are an executive in a financial company, then your technical risk acumen needs to be greater then that of an executive in a nonpublic consumer retail organization. The goal, of course, is to ensure you have enough acumen in the following five key areas:

1. Be confident in your ability to understand cross-discipline technical issues
2. Challenge the issue, resolutions, and solutions with technical people
3. Create and understand long-term strategies for business operations defense
4. Translate complex technical concepts into business terms
5. Evaluate, measure, and manage cross-discipline security plans

As a next-generation security executive, the bottom line is that you will be living in a technical world. The boundaries of cyber security/physical security/operational risk management in the relationship with technology are intrinsically intertwined. From what you are defending, to the resources you deploy to protect your business, to the issues and events you investigate, to how you manage your business—everything has a component of technology, and your success is codependent on your technical ability.

The Converging Paths of Disciplines

In the previous chapter we outlined what convergence is and why it is important. The fact remains, however, that only a small percentage of security executive