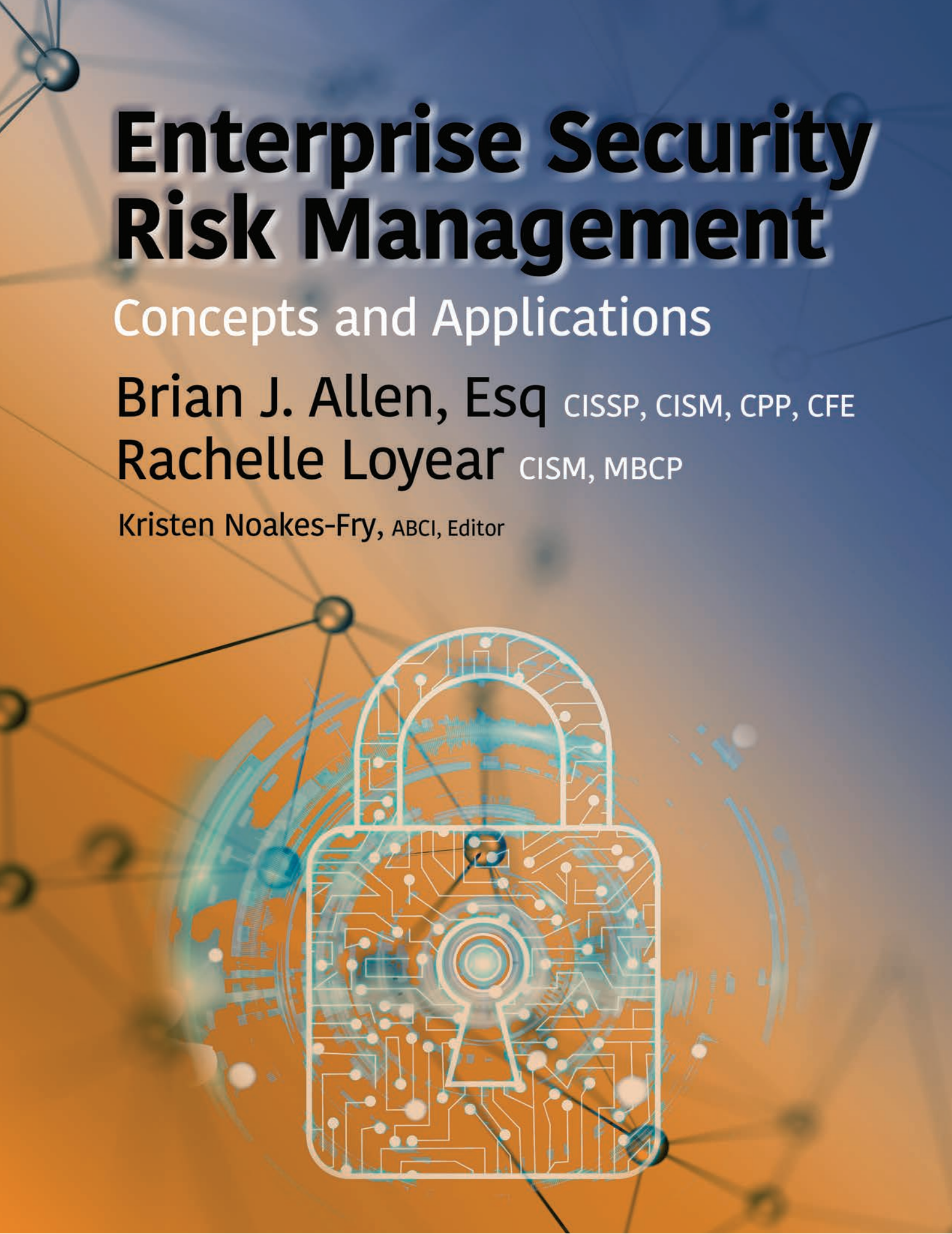
Enterprise Security Risk Management

Concepts and Applications

Brian J. Allen, Esq CISSP, CISM, CPP, CFE
Rachelle Loyear CISM, MBCP
Kristen Noakes-Fry, ABCI, Editor



EXCERPTED FROM

Enterprise Security Risk Management:

Concepts and Applications

Brian J. Allen, Esq.

CISSP, CISM, CPP, CFE

Rachelle Loyear

MBCP, AFBCI, CISM, PMP

Kristen Noakes-Fry, ABCI, Editor

ISBN 9781944480431 PDF

ISBN 9781944480424 EPUB

ISBN 9781944480448 Print

ROTHSTEIN PUBLISHING
A Division of Rothstein Associates Inc.

203.740.7400

info@rothstein.com

www.rothstein.com

Keep informed about Rothstein Publishing:

www.facebook.com/RothsteinPublishing

www.linkedin.com/company/rothsteinpublishing

www.twitter.com/rothsteinpub

ISBN 9781944480431 PDF

ISBN 9781944480424 EPUB

ISBN 9781944480448 Print

Library of Congress Control Number: 2017953266

Brookfield, Connecticut USA

203.740.7400

info@rothstein.com

www.rothstein.com

Foreword

Enterprise security risk management (ESRM) has long been in the shadows of the security industry, often mentioned but never documented. With this book, *Enterprise Security Risk Management: Concepts and Applications*, security practitioners will be able to support the growing importance of an evolving global security program for all enterprises around the world. I admire the authors, Rachelle Loyear and Brian Allen, for the work they have put in this book. It's funny how you choose your friends in life, and often they become life-long friends. In our case, we are close friends and business colleagues who all have a desire to share our knowledge with others and to lead our industry. Rachelle and Brian are two professionals with a relentless desire to help others be successful. If I had met them earlier in my career, my life would have been better for it.

Three things stand out for me as the core components of the book: enterprise, security risk, and risk principles. If nothing else, understanding these three concepts and being able to articulate what they mean in a business setting will advance your career and enhance your business acumen. If you are serious about your career and want to lead this industry, this book will help you to do that. We need leaders to take us to the next level – promoting ESRM in your organization and the business community will help to do that. From time to time, all of us have said, "If only I had known this years ago." Through this book, this is your chance to know it now and become that change agent our industry needs!

I am honored to have been selected to write this foreword. Rachelle and Brian would probably say that I mentored them. That may be partially true, but we really mentored each other. Now we are on this journey mentoring others, which is proving to be extremely rewarding as we go along this path. We have formed an

alliance called the Global Security Risk Management Alliance (www.gsrma.net/). In GSRMA, our sole purpose is to educate others on the merits of ESRM. Some readers of this foreword may know me, while others might recognize my name, since I am very active in our industry internationally and am a former President of ASIS International. I speak frequently and I am vocal advocate for ESRM in the security industry. I consider this book, the first of its kind in our industry, to be a critical component of our efforts as security professionals to protect our people and assets around the world.

Ray O'Hara, CPP

Executive Vice President at AS Solution
President and Co-founder, Global Security Risk Management Alliance
Past President, ASIS International
Las Vegas, NV
September 2017

Foreword

In their new book, *Enterprise Security Risk Management: Concepts and Applications*, Brian Allen and his coauthor Rachelle Loyear – both seasoned security professionals – present the risk and security community with new opportunities based on an evolving security management framework. Forgetting the "old school" security formulas, the authors describe the global maturation of security risk management models for businesses.

Enterprise security risk management (ESRM) leaves behind the old and limited "guns, guards and gates" constructs of what security has been to explore what security can be as a part of the overall organizational risk management framework.

I urge that all senior management read and discuss Brian and Rachelle's vision of what is possible from an organization supported by the right security risk management program positively impacting the achievement of business goals and therefore elevating shareholder value. Boards of directors, executive management, and business stakeholders will all benefit from exploring ESRM, as described in this book.

The authors describe in detail how ESRM can be applied in many areas of a company that relate to business risk, including business continuity, crisis management, cybercrime, workplace violence, cybersecurity and more. Insights will continue to be gained from the book as readers have new realizations that security risks throughout the organization have a significant positive and negative impact to the achievement of business goals.

Brian and Rachelle have presented a wealth of thought-provoking options for the reader, and I am confident that this book will add bottom line value to the companies which choose to understand and implement ESRM.

Jeff Spivey, CRISC, CPP, PSP

CEO and Founder,
Security Risk Management, Inc.
Board Director, ISACA International
Past President, ASIS International
Charlotte, NC
September 2017

Foreword

Over the years, I have become a big fan of the writings and presentations of Brian Allen and Rachelle Loyear on enterprise security risk management (ESRM). They are outstanding professionals in their field, and the information they have shared is quickly becoming required reading, at least in the circle of security professionals I hang out with. As a board member of ASIS International, I have observed how the organization appears to be using Brian and Rachelle's work to develop material for the global membership to relaunch and refocus their efforts toward ESRM.

Throughout my career, I've tried (sometimes not very successfully) to incorporate many of the principles and practices Rachelle and Brian discuss in this new book, *Enterprise Security Risk Management: Concepts and Applications*. When I met resistance within the organization, I realize now that I was not following the methodology that they describe and illustrate in the following pages. I wish I could have referred to this content about 15 years ago – I could have saved myself a lot of sleepless nights and pointless debates with folks not familiar with security or risk.

This book's understanding of what a successful ESRM program looks like is compelling and represents something we as a profession must strive to achieve. In my opinion, we're past the days when a security professional can develop a security program based on a silo approach to protecting assets. I agree that it's time to replace the views we held in the past with the approach and vision described by Rachelle and Brian. We must change our approach to security and move in the direction of ESRM, or risk becoming insignificant to our organizations in the next 5 to 10 years.

That's a strong warning, but Rachelle and Brian have realized the urgency of the situation, and you can see it in the way their explanation of ESRM unfolds. From exploratory discussions about ESRM program and what it is (and isn't) through to the ongoing maintenance and support of a successful ESRM deployment, the text really develops a methodical approach that a security professional can follow. There's no hype or drama, and their examples bring practical advice we can all use in our journey to ESRM.

If you're a security professional looking toward the future and wondering how we as a profession will succeed – read this book. If you're looking for an opportunity to broaden your understanding of how ESRM truly supports the business – read this book. And if you're looking to create your own path for future success – well, you know my thoughts.

Tim McCreight, MSc CISSP CPP CISA
Director, Strategic Alliances
Hitachi Systems Security
Member, ASIS International Board of Directors
Calgary, Alberta, Canada
September 2017

Table of Contents

3

How Can ESRM Help Your Security Program?

So far, you have seen a little bit about the basics of ESRM: What it is, what it is not, who can benefit from it, and how. Now, before we start getting into the deeper fundamentals of the practice, we want to cover some of the benefits of ESRM.

In Chapter 3, we will discuss some of the frustrations we hear from security professionals and their strategic partners across the globe, some of which you may find familiar. We will also talk about how ESRM can help alleviate many of those frustrations and at the same time, improve the overall success of your security program.

This chapter will help you to:

- Explore how security has traditionally been viewed both inside and outside of the security profession.
- Understand how ESRM can change the perception of security in your enterprise to help you better communicate the value of security risk management.
- See how ESRM is the best methodology to meet the changing global security risk climate.

3.1 The Traditional View of Security and Why the Industry Must Change

When we first began discussing and exploring the concepts and ideas that eventually led to the development of ESRM security management principles, we talked to a lot of security professionals about their programs. We discussed things like:

- What they did.
- How they did it.
- When they felt like they were being successful.
- Whether they felt supported.
- When they felt like they were not getting the job done in the way they wanted to get it done.
- If they felt valued in their companies.
- What obstacles they faced.
- What helped them to get things done.

During these discussions, we heard a lot of security professionals repeatedly express frustration with some of the same topics, even though they managed very successful programs:

- Security budgets being cut without reason.
- Projects not prioritizing security until the last minute, if at all.
- Department leaders refusing to allow security investigations in their areas.
- Clear cases of wrongdoing not dealt with appropriately.

These same themes were mentioned repeatedly by our peers in the security industry. We came to realize that much of what we considered to be wrong in our own security program, as well as what they said was wrong in theirs, had to do with the *perceptions* of security by organizational leadership – and within the security group. We began to think of that perception as the "traditional" view of security. The concepts of ESRM evolved to respond to that perception and the need to change it. ESRM is a way to help both security practitioners and business leadership understand the true role of security in an enterprise. All this builds the trust needed to truly make security an integral part of an enterprise and help the organization carry out its mission of managing security risk.

3.1.1 The Traditional View of Security

Here is an exercise that we did repeatedly. Try it. We think you will be surprised at the results. The next time you are in a room full of security professionals, ask this deceptively simple question:

"What does security do?"

3.1.1.1 What Does Security Do? – The Answer from the Security Practitioner

Chances are, you will get as many different responses as there are people in the room. Here are just a few of the kinds of comments we heard, and similar to what you are likely to hear during the discussion:

- "Security's job is to protect the company's business assets."
- "Information security – making sure sensitive personal information, like credit card data, is protected."
- "We're focused on physical security."
- "Investigating breaches of company security policy."

These responses are not wrong, exactly. In fact, with the traditional way of approaching security, they are all correct – specifically to the person talking – and that is the heart of the problem. The answers are all

very different, and they are all *incomplete* as a definition of the security *profession*. That is because they are all describing security *jobs*.

The other problem with these types of common answers is that they do not touch on what the role of security is – only what the answerer *sees* security do. The definitions feel like they are incomplete because they do not start with and consistently define the role of security – they just talk about tasks.

Questions for the Security Practitioner

- "Have I ever asked stakeholders in my organization an open-ended question like, 'What is security's role here?'"
- What would the answers be like if I did? Would they vary, by department or title?
- "What benefit might I get, both from asking the question and from the answers?"
- "How would I answer if someone asked me the same question? Would my answer change, depending on the circumstances (for example, who was asking the question)? Would I just be listing the tasks that my security program performs? Or would I have a broader answer describing my role in the company?

3.1.1.2 What Does Security Do? – The Answer from the Board of Directors and Senior Executives

Now imagine you left that room full of security professionals and walked next door to ask the same question of a group of board members, line-of-business owners, or senior executives. You would almost certainly get an equally wide-ranging, equally "correct" – and equally incomplete – set of answers, perhaps like:

- "Security manages the physical security on our property, like the guards and gates."
- "Security protects our data, through things like password management and network monitoring."
- "It is all about protecting our people on campus, and making sure our systems and data are safe."
- "They help keep us up and running if something goes really wrong, like a natural disaster."

Again, these answers, in and of themselves, are not wrong. They are based on these key decision-makers' perceptions, their mindset, their experiences, and what they observe security doing every day. But, just like the security practitioners' responses, these are not adequate to define what security is. The ESRM definition of security and our role goes beyond what we see in both sets of answers above, not simply describing the tasks we are responsible for, but clarifying security's role in the enterprise overall.

3.1.2 Why the Security Industry Needs to Define "Security"

Reactions like the ones we have listed above clearly do not reflect a comprehensive, accurate view of the important work you do – and we imagine they do not reflect the way you want yourself and your role as a security professional to be perceived. But they are all too common, and they are damaging to your effectiveness, and your success, as a security professional.

That is why defining security – its role, its objectives, and the most appropriate ways of measuring success – is so important. If we in the security profession cannot define what we do, how we do it, and why we do it, we:

1. Cannot possibly be sure we are successful.
2. Cannot ensure that security is recognized seriously as a serious professional business discipline.
3. Will be leaving it to others to define security through their perceptions and experiences (and define it in ways that we are not likely to agree with).

Significant issues can come from letting people outside the security organization define security:

1. It often results in the security practice within an enterprise being broken up, or "siloed," so physical and investigative security responsibilities are handled separately from information/cybersecurity responsibilities (although when you are using ESRM as your security philosophy, the process of protecting assets, whether they are physical or logical, is precisely the same).
2. It can lead to some clear security responsibilities being handled by groups entirely outside of security (for example, HR performing investigations or facilities handling guard services).
3. It can lead to security functions being cut from areas where it is assigned as a responsibility but is not central to the core department mission, and then the enterprise misses key aspects of a comprehensive security program entirely.

Why, then, do security practitioners, business executives, operational managers, and ordinary employees still have so many different answers to the question of what security is, and such different expectations of what the security department should be doing? To us, the answer lies in several problems we have discussed already in Part 1 of this book and will continue to focus on going forward. They are:

- The absence of a consistent "philosophy" of security management.
- A focus on tactical functions – daily operational tasks – rather than strategic, risk-focused, decision-making that leads to our programs being defined by those functions and assigned tasks.
- A view of the security practitioner's role that centers on enforcement of rules, rather than on management of risks.

These problems can lead to weakened security that can compromise the enterprise and lead to frustration for both security practitioners and their strategic partners in the organization. They can all be addressed mostly effectively by the application of ESRM principles.

3.1.3 The ESRM View of Security – A Profession, not a Trade

In this book, we will be taking a close look at that deceptively simple question, "What does security do?" The varying responses and reactions we saw when security practitioners and enterprise leaders were asked to define security suggests that it is a difficult question, but it really is not. At least, not when ESRM principles are applied. ESRM offers a very simple, highly definitive, and extremely useful answer:

"Security manages the enterprise's security risks – all of them – using basic risk principles."

Looking back at the earlier exercise of asking, "What does security do?" to a roomful of security professionals, we can see that – whether they recognize it or not – their responses to the question can be distilled down to, "Manages security risks."

Table 3-1 shows what their statements mean when they are looked at through the lens of ESRM. The bottom line always comes back to a risk that needs to be managed through sound risk management principles.

Table 3-1. Traditional Views of Security Reconsidered Through ESRM

Traditional View	ESRM View
"Security's job is to protect the company's business assets."	To be precise, security means protecting the company's assets – all of them, physical, logical, and human – against the many risks presented by a fast-changing and increasingly dangerous world. All the security measures we take are aimed at managing and mitigating known and emerging risks.
"Information security makes sure that sensitive personal information, like credit card numbers, is protected."	A seemingly endless series of high-profile data security breaches shows the risks of inadequate information security – risks that can literally be fatal for a enterprise. ESRM principles recognize the entire range of security risks, and help security professionals and their strategic partners in the enterprise address them appropriately while understanding each other's roles in the management process.
"We're focused on physical security."	Physical security is the practice of protecting the company's physical property from a variety of security risks, ranging from theft to damage to misuse. The ESRM approach, however, views this as an aspect of risk. Those physical security activities being done are there to *mitigate a risk or multiple risks*, not just done for the sake of doing them.
"Investigating breaches of company security policy."	When security policies are not followed, whether intentionally or unintentionally, the company is exposed to an enormous range of risks, ranging from legal liability to fines for regulatory noncompliance to reputational and brand damage. Investigation is the first, necessary response to an indication of a breach of policy. It is also the first step in understanding root causes and mitigating the risk(s) involved.

3.1.3.1. Managing Security Risks

Managing security risks enterprise-wide is your role and your responsibility as a security professional. ESRM, because it is comprehensive, holistic, and all-encompassing, is what makes that possible. Because no matter what type of security risk is being discussed, the practice of managing those security risks is essentially the same. Treating all security risks in the same manner will mean your program is completely consistent in its approach to, execution of, and messaging about all parts of the security program. Describing what you do to manage security risks will close gaps in awareness of how you are perceived by your peers inside the organization. This consistency makes it easier for others both to understand what you do and to be more willing to partner with you in protecting the enterprise.

3.1.4 ESRM-Based Security – Moving from Task Management to Risk Management

At the heart of ESRM is the recognition that security is an *overarching strategic concern*, not a set of tactical, operational tasks to be performed.

3.1.4.1 Security Task Management

In today's security world, every practitioner is busy. There are threats to monitor, video cameras to repair, investigations starting up, gates to guard, executives to protect, data to encrypt, metrics to analyze and report on, and employees to manage. So, it is not surprising, as we saw earlier in our "questions" exercise, that the tasks we perform every day are used to define our discipline. These are the first things that come to mind when we are asked to explain what we do for the organization. It is not surprising, but it is a

mistake. It is a mistake that damages our effectiveness and credibility as security professionals and, even more importantly, compromises the security of the people and assets we are tasked with protecting.

Why? Because when you define your role as doing things – completing tasks – then it is easy for people to view that task as unimportant, or not their problem, or not something that should come out of their budget. It is just one task or item, after all. But ESRM can change that definition by ensuring that your role is clearly defined as managing security risks. Describing your role as managing risks means that those risks must at least be *considered* when security decisions are made, or else the decision makers are not performing due diligence to protect their operations, or even more simply, are not making educated security decisions about their assets.

3.1.4.2 Security Risk Management

Risk management is the identification, assessment, treatment, and monitoring of security risks to the organization. It is fundamentally different from task management because it means looking at ways to protect the company at a strategic level, as well as at a tactical level. It is deeply concerned with allowing the enterprise to complete its mission with minimal interruption from security-related incidents. Of course, risk management can still involve tasks, but these are tasks with a higher purpose. These are tasks that are given to personnel with tactical security expertise so that they can mitigate an identified risk. In this way, the role of the security group is to carry out a program that helps the enterprise to protect itself, not merely to be a gate or a guard or an access control method. This may seem like playing with words, but truly this small difference in approach can lead to a very big change in the way you, and your security team are perceived.

3.1.4.3 The ESRM Solution: A New Philosophy

Implementing ESRM brings with it a holistic view of securing the enterprise through a consistent philosophy and management methodology. This view extends far beyond the day-to-day operational tasks that are assigned to the security organization.

It seems obvious, and yet many security professionals routinely do these tasks – assess risks and implement risk mitigation plans, perform root cause analysis, make proactive recommendations – without considering that they are, in fact, aspects of overall, enterprise-wide security risk management. That lack of consideration about how the tasks impact overall risk means that moving from a task-oriented, performance-based security program to a comprehensive, holistic ESRM program requires a *fundamental* shift in how many security professionals think about both security and risk. It also requires a shift in how they think about how their current responsibilities fit with the overarching role that security plays in the enterprise. When we, as security professionals, change the way we think, we change the way we present ourselves, and it follows that we also change how others see us – from task-doers to risk managers.

3.1.5 Why Is the Traditional Approach to Security So Frustrating for So Many People?

One of the most critical issues we have found in our discussions with our peers in the security profession and with their strategic partners inside their organizations is that almost everyone involved with security (whether the practitioner or the impacted stakeholder) often feels frustration at the process and the experience. This frustration can manifest in many ways. For example, an internal business partner has overturned or dismissed a security proposal, the security requirements have been dictated to the security practitioner against their recommendation, or a business leader has decided that security requirements are onerous and interfering with getting their work done.

When we looked at all the various frustrations, however, we found that they are often the result of one of two things:

1. The security practitioner is not fully aware of what their role is.
2. The strategic partner is not fully aware of what security's role is.

Both situations are avoidable and are the responsibility of the security practitioner to correct. First, by understanding that the role of security in the enterprise is to be mangers of security risk. Second, by communicating a comprehensive understanding of that role and appropriately setting the expectations of what security and the business leaders should be doing in the security risk management process.

3.1.5.1 The Missing Network Switch: A Story of Security Frustration

Let us look at a fictional story to examine this all-too-familiar problem from the perspective of both the security practitioner and a business function leader. Although this is fictional, it is something that happens in real life all too often. In the next two sections, we will examine a security risk and incident as played out in the "traditional" security environment.

3.1.5.1.1 The Traditional Security Environment

The Security Practitioner

Rick M., is a security manager for Aspect Insurance, a multibillion-dollar health insurance provider. Rick has been assigned the task of protecting one of his company's data centers, which is undergoing a major upgrade involving an independent contractor. Data security is a critical concern for the company because its operations are subject to rigorous regulatory compliance requirements. The data center handles massive amounts of personally identifiable information, and a security breach would be a disaster, exposing the company to regulatory scrutiny, legal liability, and serious reputational damage to its brand.

Rick knows all this, and he is deeply concerned about the security risks inherent in having outside contractors onsite in such a sensitive location. In keeping with established industry best practices, he recommends that the company conduct background checks for all the contractor's employees involved in the project.

When the data center's facility and finance managers see the plan and the associated costs, they are not convinced that it is necessary or worth the cost, since the cost is not covered in the project budget and would require that they find new funding. They also do not see the issue as "their problem." To them, personnel security is somebody else's concern. The company has technical solutions for Information Security with intrusion detection and prevention technologies, all managed by IT. The facility and finance managers point to that and to the physical security measures that are already in place – guards and gates, video cameras and card readers – so they do not see the need for more. They reject Rick's recommendations.

Rick comes away from his presentation feeling that his expertise is not being valued and that he is not being allowed to do what he was hired to do: protect the company. More significantly, he comes away still concerned about the security of the data center – and it does not take long for his fears to be realized.

Three months after his presentation, a network switch is stolen from a server rack in the data center by a contracted employee (whom they later learn has burglary convictions on

his record). The switch is valued at only a few thousand dollars, but during the theft, several active servers are badly damaged, and months of critical data has been compromised. The data is possibly destroyed. Also, it could have been possibly copied, stolen, and then corrupted to hide the data theft – for which the stolen network switch could even have been a cover! All the elaborate cybersecurity measures the company had put into place were meaningless because someone simply walked into the data center with a malicious intent.

When he learns of the incident, Rick has an "I told you so" moment. (Of course, as a professional, he keeps it to himself.) But his sense of satisfaction does not last long, since, as the security manager, he is the one held responsible for letting the intrusion happen. He begins an investigation and quickly identifies an employee of the independent contractor who was onsite at the same time as the theft. But by then, the employee is no longer working for the contractor, who claims to have no knowledge of his whereabouts.

The Business Function Leader

Paul K. is the network and systems vice president responsible for the systems that were damaged in the theft of the network switch. His team is under intense pressure to repair the damage, get the servers back up and running, and determine whether the data was destroyed (which would be a bad outcome) or stolen (which would be even worse). He must also determine whether any of the compromised data was covered by mandatory reporting regulations. If he cannot definitively establish that the data was not stolen, he must begin the reporting process for a potential violation. Additionally, while this is going on he must restore regular business operations and must recover the lost data, some of which was not backed up real-time and will have to be re-created from scratch. Angry at what he sees as a clear security failure, Paul calls Rick in and demands to know what went wrong and why.

Rick explains that the theft could have been prevented if the background checks he recommended had been in place – checks that the facility and finance manager at the data center rejected because they were too expensive. Instead of being appeased by this, Paul is now angrier than ever. He accuses Rick of not fighting hard enough for the security controls he believed were necessary – and that, by not fighting harder for those controls, he has not done his job. Rick was tasked with protecting the data center, and, from Paul's perspective, he obviously failed to do that.

At the end of this story, both Rick and Paul are unhappy and frustrated at the security organization's seeming inability to "get things done." And the main reason for their frustration, and for the security failure that brought it to a head, is a fundamental, and very common, situation: A security professional was given the responsibility to undertake an assignment but not the means to carry it out.

These problems – both the security failure and the frustration and "blame game" that go along with them – could have been prevented by the application of ESRM principles. In the next section, we will look at how this situation might have played out in a company, and a security organization that based its decision on the ESRM philosophy.

3.1.5.1.2 The ESRM Security Environment

The Security Practitioner

When Rick is tasked with "protecting" the data center, he views the assignment not simply as a security problem to be solved, but as a security risk issue to be managed. He begins by identifying the serious risks – regulatory, legal, and reputational – that the company would face in the event of a security failure during the data center upgrade. Then he identifies the key stakeholders who would be impacted by a security failure and realizes that they include an extraordinarily broad range of roles and organizations within the company. (One of the most important is the risk of regulatory violations if the data has been stolen.) For that reason, instead of presenting his recommendations for background checks on all the independent contractor's employees, Rick goes to where he believes the risk *lives*: first to Paul, the network and systems vice president and then to the General Counsel, who would own the regulatory risk.

The Business Function Leader

At first, Paul does not understand why Rick has come to him about background checks, since the facility and finance managers have already said they believe Rick's recommendations will be too expensive. But when Rick lays out in detail the possible consequences of a security failure, Paul sees that the risks would, in fact, impact him directly, far more than either facilities or finance. He decides that the risks are unacceptable to his network and data security, and that the costs of background checks are small compared to his data security risks. He brings in the human resources (HR) and legal departments, and asks Rick to collaborate with them in designing and conducting background checks on all the independent contractor's employees assigned to the project. Rick and Paul are both satisfied: Paul is because his risk is mitigated, and Rick is because the correct risk owner made the risk mitigation decisions.

3.1.5.1.3 The ESRM Difference

Our scenario, as we left it above, could have two different endings:

1. The background checks could reveal that several of the employees who the contractor was planning to have onsite in the data center had misrepresented their employment histories, some had exaggerated their technical qualifications – and one had an extensive criminal record. The contractor would immediately remove those employees from the project, and the network switch would never be stolen, or the data compromised, because the thief was never allowed into the data center.
2. Events could have played out differently. Paul might have listened, understood the risk, and still chosen not to accept the additional project costs of background checks, and the theft and damage might still have occurred.

Crucially though, with ESRM principles in place:

- The responsibility for the security risk would have resided in the appropriate place – with the owner of the business assets at risk.
- Paul, as an executive, would have been on record as accepting the security risk.
- It would have been difficult, if not impossible, for anyone to lay the blame on Rick or the security organization, because it was clear that it was Paul who owned the risk and made an educated risk decision.

This fundamental concept – the acceptance of risk by its true owner – is an essential component of ESRM. As security professionals, we know that security incidents are always going to happen.

Information assets will be lost, physical assets will be stolen or damaged, and business processes will be interrupted. There is no such thing as perfect security, and there never will be. However, we believe that when security professionals are not practicing ESRM as the basis of their security program, the wrong people can often be making security and risk decisions, whether based on right information and criteria or not.

Most often we see that they are the wrong decision-makers, not because they should have no say in the decision, but because they are not the *sole* asset owner or stakeholder, and they should not have the *only* say. Sometimes, as we saw in the example above of a function or department making a security decision based solely on financial details, the decision maker is not a true stakeholder in the *risk* at all.

Unfortunately, when things go wrong, as they inevitably will, it is the security professional who often takes the blame. This blame was mostly because there was no clearly defined understanding of what the security practitioner's role was in the first place. ESRM principles, however, can significantly reduce the number of stories like Rick's and Paul's by shifting the security practitioner's defined role from task management to risk management.

Questions for the Security Practitioner

- "What is the source of frustration in my role as a security practitioner?"
- "Are my recommendations being accepted and implemented? If not, why not?"
- "Can I be more involved in the security decision process?"

3.2 The Evolving Global Risk Environment is Driving Industry to Risk Management Postures

As members of the security profession, we driven to focus on risk management rather than simple security tasks by the rapidly changing security risk situation across the globe. Technology, globalization, social media, rapid change, and faster travel make us all much closer together than we used to be, and these changes increase the potential for business disruption. ESRM incorporates a flexible response to this changing environment because continually assessing and managing risk puts you in a better position to respond quickly to security incidents, whether anticipated or unforeseen.

3.2.1 Security and Risk Threats are Real

The security and risk issues that will be discussed in this book – the issues that ESRM addresses – can threaten an enterprise's competitiveness, its profitability, and even its very survival. In the year 2014, data breaches like the ones at Target, JPMorgan Chase, and eBay compromised the sensitive personal data of millions of people, exposing them to the possibility of identity theft and other kinds of fraud (Roman, 2014). These security breaches cost those enterprises millions of dollars, as well as damage to reputation and brand that, while difficult to calculate precisely in dollar terms, was probably even worse. Board members and senior executives can face lawsuits, regulatory liability, even criminal charges if they fail to protect the interests of shareholders, customers, and employees. Damage to physical infrastructure (factories, roads, bridges), like the catastrophic destruction caused by the earthquake and tsunami that struck Japan in 2011, can disrupt supply chains, forcing factories and stores thousands of miles away to close. The workplace violence that is now all too common threatens not only employees' lives, but also their morale and their productivity. Even small-scale problems, like employee theft, can seriously impact an enterprise's bottom line.

In Table 3-2 below, we show just a few examples from the 2016 annual global risk report from the World Economic Forum. Many of today's critical risks include terrorism, random acts of violence, fraud, natural disasters, and – especially prevalent in the evolving security environment – cyber-attacks and other kinds of information security risks. We have included the risks from this report that we consider especially applicable to security professionals, but we encourage you to visit the WEF site for risk trend awareness.

Table 3-2. Global Risks by Category

Category	Risk
Economic	• Failure/shortfall of critical infrastructure. • Illicit trade (e.g. illicit financial flow, tax evasion, human trafficking, organized crime, etc.).
Environmental	• Extreme weather events (e.g. floods, storms, etc.). • Major natural catastrophes (e.g. earthquake, tsunami, volcanic eruption, geomagnetic storms). • Man-made environmental catastrophes (e.g. oil spill, radioactive contamination, etc.).
Geopolitical	• Failure of national governance (e.g. failure of rule of law, corruption, political deadlock, etc.). • Large-scale terrorist attacks. • State collapse or crisis (e.g. civil conflict, military coup, failed states, etc.).
Societal	• Large-scale involuntary migration. • Profound social instability.
Technological	• Adverse consequences of technological advances. • Breakdown of critical information infrastructure and networks. • Large-scale cyberattacks. • Massive incidents of data fraud/theft.

Source: World Economic Forum (2016), *Global Risks Report,* pp. 85-86.

The reality is, the security and risk issues we will be talking about throughout this book are virtually life-or-death questions – for people and for enterprises.

3.2.2 The Risk Conversation is Changing Rapidly

The world is a rapidly changing place, and the pace of change is getting faster each year. Risk items that have the utmost importance and impact in one year are supplanted the next year by new and different threats. We cannot tell exactly what the future of security will hold, but we can predict with a measure of certainty that it will be different from what we know now, and likely will different from anything we can imagine today. That shifting ground is what makes the conversation about risk and risk management so important in today's security realm. Tasks, technologies, standards, practices, and skills can become obsolete, but risk is a constant threat. Being able to understand risk, examine environments, and discover how they are vulnerable to harm, are skills that will never be obsolete, even in a rapidly changing world.

While the future of security is unknowable, we certainly can say that as a security professional, embracing an ESRM philosophy will make you and your security program:

- More nimble.
- Quicker to become aware of new threats and risks.
- More able to respond to changing environments.
- Better positioned to assist the enterprise in responding to threats of harm to the business.

3.3 What Does "Security Success" Look Like?

Here, we will take a moment to discuss what security success means in the context of this book. We all want our security efforts to be successful, and of course we all want successful security careers. But security success is not necessarily easy to define, or even to recognize. That is a genuine problem, because if we do not know what success looks like, we can never be sure we have achieved it.

To explore this, try a simple thought experiment:

> You have been put in charge of setting up a brand-new security program for your entire company. When you are six months in, the senior executives who gave you that responsibility want to know whether the program is a success. How will you determine how successful the program has been so far, and how will you communicate your conclusions to those high-level decision-makers?

3.3.1 Success is Not Just Measured by Numbers

Maybe you will look for key performance metrics. Those metrics could measure anything from the number of investigations your organization has conducted, to the dollar value of the reduction in losses from fraud. They could represent the number of intrusion attempts that you have intercepted. Or maybe they would show a reduction – or at least rationalization – of your security budget because the right people with the right skillsets were assigned to the right tasks, and some previously manual tasks were automated. Those are all great data points, and they are all useful, even necessary. But do any of those numbers, individually or in the aggregate, really define "success?" We do not think so.

They are necessary because they define scope, scale, efficiency, and effectiveness, all of which are important. However, they do not communicate whether a risk tolerance threshold has been clearly established by the appropriate stakeholders. Nor do those numbers measure and communicate a changed threat level that exceeds the set tolerance in a way which would require the business to adapt the mitigation approach for any specific risk. That is why, in this book, we will present a novel approach to defining the success of your security program.

3.3.2 In Security Success, Intangibles are Important

ESRM success – not just security success – is measured at least as much by intangibles as by those metrics above. To figure out what those intangibles are, it is imperative to assess your current processes and your overall approach to how you practice your security responsibilities and finally to determine how that practice is perceived in your environment.

Here are a few questions to consider when making that assessment:

- "Do my counterparts in the business see me as a true partner?"
- "Is leadership including me at the beginning of new projects, to help identify risks and develop mitigation plans from the outset?"
- "When changes in business processes and business models are being considered, am I involved?"
- "Do the metrics and reports that I send out truly align with security risks and my strategic partners' concerns?"

Success is not just a question of how well your organization is performing (which is, of course, important). It is also about how much personal and professional satisfaction you are taking in your role as a security practitioner.

You should also be asking yourself some fundamental questions about how you feel about your job:

- "Do I truly feel valued by my superiors, my security colleagues, and my peers in the enterprise?"
- "Does the company offer me the career path I desire? Am I doing everything I can to advance along that path?"
- "Am I communicating the importance of what I do?"

3.3.3 Your Answers Create Your Definition of "Success"

There is an important reason we have based our definition of success on questions – and your individual answers to those questions. As much as you might like a straightforward way of defining your goals and determining whether you have achieved them, it is not that simple. It is a little like a child asking a parent, "When will I be a grownup?" It is easy to reply, "When you are eighteen years old," or "When you are at least five feet eleven inches tall." But, as is so often the case, the easy answer is not necessarily the right one. As we all know, lots of grownups are not five feet eleven, and lots of people over eighteen (or thirty, or even fifty) are not really grownups.

Questions for the Security Practitioner

- "What does success really mean to me? Is it in the form of a promotion, a higher salary, a bigger budget, more responsibility – or is it simply that my work is more satisfying?"
- "Do my colleagues in the security organization, my manager, and my business partners see security success the same way I do? If not, what can I do to make our perceptions align better?"
- "Are we on a path to properly recognize security's role in the organization, and gaining the necessary partnerships and respect to be successful?"

Your ESRM program will not be perfect from day one. (In fact, it will never be perfect, and recognizing that fact is a key component of being able to define success realistically.) Furthermore, it will not be measured by security or risk metrics, at least not in the meaningful way that ESRM requires. How will you know when you are successful? In some ways, it is like trying to define how mature you are. How mature is your organization? How mature are you at your security craft? How mature do you need to be or want to be, so that you can accomplish your personal and professional goals? Of course, even when you feel like you have matured – either you individually, or your entire program – it always feels like there is room for improvement.

ESRM is, in fact, a process of continuous improvement. As your security program becomes more successful, your strategic partners will rely on you more, and you will know you are doing what needs to be done. That is part of what success looks like – always recognizing that there is more to be done.

A good benchmark question for a security professional would be:

"Is our security program or my individual practice more mature today than it was yesterday?"

The answer will not be based on how many viruses you have blocked or how many dollars you have saved with your guard contract. It will be far more meaningful than that.

3.3.4 The Security Professional and the Business Leader: Using ESRM to Move Beyond Frustration to Success

As previously discussed, it can be frustrating when the business does not accept our decisions, our recommendations, or the plans we are trying to implement. And security can be every bit as frustrating for business leaders, who often see it as an obstacle to getting things done. Part of the problem, of course, is that business leaders do not necessarily recognize the importance of what we do and what we are trying to do. To put the problem in its simplest terms, they do not recognize our role in the enterprise.
ESRM will help us gain recognition because we, as the security professionals, also have a responsibility to recognize what our role is, and what it is not. In ESRM, at its most basic, we learn that our role is simply to manage security risk. That means guiding the business through the risk decision-making process, not making the decisions ourselves.

It is vital that we, as security practitioners, recognize that this is not avoiding responsibility or shifting blame. In an ESRM environment, our value as security practitioners comes from guiding our strategic partners in the organization through a proper decision-making process about the security risks to their business assets. That aspect of ESRM allows us to build the true partnerships, enabling us to succeed in the mission of protecting those assets the business deems important to protect.

There are two sides to this process:
1. Helping the business understand security.
2. Helping security understand the business.

The place to start with both sides of the process is understanding what your enterprise internal partners want and need from you. You can best do that by the simplest means possible: asking them. We will talk in Chapter 4 about how to do just that.

The payoff for the security practitioners comes when the business recognizes the true value of security and embraces it as something that adds real-world business value. This recognition reduces that frustration we have all experienced and makes the overall security program more successful.

Questions for the Security Practitioner

- "Do my colleagues in the security organization view their role the same way I do mine?"
- "Do we base our view on the business priorities of the enterprise? If not, why not?"
- "Is security updated regularly to address changing business needs?"
- "How often does the whole enterprise review its business priorities, and how often (if at all) are those priorities communicated to the security organization?"
- "Are you and the rest of the security organization properly aligned with the business? If not, why not?"

3.3.5 The ESRM Philosophy of Security Success

In 2010, ASIS International's CSO Roundtable conducted a benchmarking study of security professionals to determine the extent to which ESRM concepts were being accepted in the security and business communities. Comments by professionals participating in the study show that ESRM principles are very much top-of-mind for both security and business executives.

- According to Timothy Williams, Director of Global Security, Caterpillar, "With ESRM's holistic approach to security came the understanding that a whole host of business issues that were not

traditionally associated with "security" – think, for example, of Sarbanes-Oxley or HIPAA – were now firmly part of security's bailiwick, underscoring again how important it is for security professionals to be business professionals first" (CSO Round Table, 2010, p. 3).

- Dr. Erwann O. Michel-Kerjan, Managing Director, Risk Management and Decision Processes Center, The Wharton School of the University of Pennsylvania, explains, "The growing recognition of Enterprise Security Risk Management (ESRM) as a holistic view of risk – all risks – throughout an organization is important; this holistic view helps ensure that the threats that might typically not be recognized in an enterprise risk management program focusing primarily on financial risks (such overlooked risks, for example, might include: risks to brand and reputation; physical supply-chain risks; or loss of consumer confidence if your data is stolen or networks attacked) are now more and more fully identified, prioritized, and mitigated" (CSO Round Table, 2010, p. 5).

These comments, and many others from security and business thought-leaders, show an emerging consensus that ESRM is necessary for security success – now and in an increasingly complex and dangerous future. Central to ESRM is the recognition that security success is simply, business success.

As a security professional, you are operating in an environment driven, for the most part, by profit and value. This is not the whole story, of course. For example, there are government and nonprofit organizations that are not profit-making entities, and even many private-sector businesses that have goals other than profit (such as, contributing to the wellbeing of their employees or their communities). But most enterprises, certainly, are interested in protecting and increasing the value they deliver to their owners, their shareholders, their customers, and others. Every enterprise, whatever its mission, has a critical interest in protecting the assets it views as important. These two points come together in the ESRM philosophy, and understanding them and applying them is crucial to your success as a security professional.

Questions for the Security Practitioner

- "Looking five years into the future, what role do I see ESRM playing in my success as a security professional?"
- "How can ESRM help me identify the strategic partners who will be critical to my success? How can I communicate and collaborate more effectively with them?"

3.3.5.1 Security Becomes Strategic

The ESRM philosophy can be considered fully in place when basic risk management principles are accepted throughout the entire security program and when those principles mesh consistently and comprehensively into the daily thought processes of all the security practitioners in the department. Over time, this change will mature how the security organization functions and will turn security managers into security and risk professionals. Just as importantly, it will change the perceptions of other stakeholders across the enterprise – including internal business partners, senior executives and board members. That means the difference between being defined as a tactical, operational problem-solver, to being regarded, eventually, as a strategic partner.

3.3.5.2 Security Becomes a Business Function

We are focused on risk management as a philosophy, but we are not suggesting that security management doesn't also involve managing operational tasks or implementing security processes and systems. It always has, and it always will. Nevertheless, security task management becomes ESRM when those security processes and systems are put in place, enterprise-wide, according to a strategic framework of risk mitigation and response, developed with input from business function leaders. Those leaders are the people with the most at stake in protecting those assets; they are ones who must take responsibility for them; and they are the ones who must decide on the return on investment (ROI) of any risk mitigation plan. The risk treatment plan that is chosen may be – almost certainly will be – assigned to the security organization to implement and manage. But the plan itself will be the result of a carefully considered business decision. Embracing ESRM means ensuring that security is a *business function*, based on a clear-eyed understanding of business risk. When we see security as a business function like any other – one that delivers real-world business benefits – our strategic partners will see it the same way.

Questions for the Security Practitioner

- "When a task is assigned to me, or when I assign a task to someone else, does everyone involved clearly understand why the task is important, what asset is being protected, how that asset impacts the business, who and what will be impacted by it, and what standard of performance is expected?"
- "Is our understanding of an assigned task based on a common, consistent philosophy that is clearly understood by both the security organization and our business partners?"

Chapter Review

In Chapter 3, you learned:

- Security professionals and other business professionals do not always agree on what "security" is or understand the role of the security professional in the larger organization.
- ESRM is a path to managing security risk in an ever-changing global risk environment.
- Measuring the success of a security program is complex and will mean different things to different people and organizations. The ESRM philosophy can help the security practitioner understand their own program's best measure of success and meet it.

Looking Forward

In Part 2 of this book, we will:

- Begin an in-depth discussion of all the steps of the ESRM life cycle and look at the best practices surrounding an ESRM implementation.

Practitioner steps before moving on to Part 2:

- ✓ In your own words, answer the question, "What does security do?"
- ✓ Ask some of your business partners and executives the question, "What does security do?" What answers did you get?
- ✓ Think about some of the new risks your organization will face in the changing security environment.

Security Program Self-Assessment

In this self-assessment, you should think about the answer to the questions posed, and then see where your program is on the identified ESRM spectrum.

Question	Y/N	Is This ESRM?
Do you understand what your enterprise requires to consider your security program a success?	□Yes □No	**NO**: If you have never explored the benchmarks of success for your program, this is a preliminary step for an ESRM program. **PARTIAL**: If you have some metrics identified to define success, but they involve documenting tasks and metrics based on efficiency, you are part of the way to an ESRM implementation. **YES**: If you have specific understandings with your strategic partners regarding the risks you manage and your role, as well as methods to measure adherence to the risk tolerance, you are practicing ESRM.

Questions for Discussion

1. What security issues can you think of that might be caused by operating security in corporate "silos?" Are there benefits to silos that could outweigh these issues? What do you think?
2. Can you identify three security tasks that could be operationalized to free up time and resources to address strategic risk issues? How might this impact the business?
3. How could you communicate ESRM principles and their importance to your peers, both inside and outside the security organization?

References

CSO Roundtable of ASIS International. (2010, April). *Enterprise security risk management: How great risks lead to great deeds.* Retrieved from https://cso.asisonline.org/esrm/Documents/CSORT_ESRM_whitepaper_%20pt%201.pdf

Roman, J. (2014, December 30). Top data breaches of 2014, infographic: Lessons learned from year's top incidents, *Bank Info Security.* Retrieved from http://www.bankinfosecurity.com/top-data-breaches-2014-a-7736

World Economic Forum. (2016). *The global risks report 2016*. Retrieved from http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf

Learn More About It

For further reading about security management:

Walters, D., Fischer, R. J., & Halibozek, E. P. (2013). *Introduction to security*. Burlington, MA: Butterworth-Heinemann.

Fay, J. (2011). *Contemporary security management*. Burlington, MA: Butterworth-Heinemann.

About the Authors

Brian J. Allen, **Esq. CISSP, CISM, CPP, CFE** has more than 20 years' experience in virtually every aspect of the security field and is founder of the Security Risk Governance Group (www.esrm.info), an executive advisory firm that provides security management solutions and implements enterprise security risk management (ESRM). Previously, as Chief Security Officer (CSO) of Time Warner Cable (TWC), he was responsible for protecting TWC's assets worldwide. He coordinated TWC's crisis management and business continuity management (BCM) programs, managed the cybersecurity policy, and led the security risk management program. In addition, he managed TWC's security policy and relations with law enforcement and government authorities, as well as all customer security risk issues, oversaw internal and external investigations, and headed the company's workplace violence program. Before joining TWC in January 2002, he was Director of the Office of Cable Signal Theft at the National Cable and Telecommunications Association, Washington, DC, and the owner of ACI Investigations, a provider of security guard, investigative, and consulting services.

Brian earned his Bachelor of Science degree in criminal justice from Long Island University and received his Juris Doctor degree from Touro Law Center in New York. He is a member of the New York State Bar Association, a Certified Protection Professional (CPP) with ASIS, a Certified Information Systems Security Professional (CISSP) with ISC2, a Certified Fraud Examiner (CFE) with the ACFE and a Certified Information Security Manager (CISM) with ISACA. Brian is also a member of the International Security Management Association and the Association of Threat Assessment Professionals.

Brian is an Adjunct Professor at the University of Connecticut, School of Business MBA Program and is active in industry organizations. He served as a member of the Communications Infrastructure Reliability and Interoperability Council (CSRIC), an FCC appointed position, and co-chaired its working group on Cybersecurity Best Practices and the Cybersecurity Framework. He is one of four elected communications company representatives to serve on the Executive Committee of the US Communications Sector Coordinating Council (CSCC). He works with the Cross Sector Cybersecurity

Working Group, established by the U.S. Department of Homeland Security (DHS) under the Critical Infrastructure Partnership Advisory Council. Brian has served on the board of directors of ASIS International, and the board of trustees of ASIS International's Foundation. He is currently a member of the Board of Directors of the Domestic Violence Crisis Center in Connecticut.

With Rachelle Loyear, he co-authored *The Manager's Guide to Enterprise Security Risk Management: Essentials of Risk-Based Security* (Rothstein Publishing, 2016).

Rachelle Loyear, **MBCP, AFBCI, CISM, PMP,** has spent over a decade managing various projects and programs in corporate security organizations, focusing strongly on business continuity and organizational resilience. In her work life, she has directed teams responsible for ensuring resilience in the face of many different types of security risks, both physical and logical. Her responsibilities have included: Security/business continuity management program design and development; crisis management and emergency response planning; functional and location-based recovery and continuity planning; training personnel in crisis management and continuity; operational continuity exercises; logistical programs, such as public/private partnership relationship management; and crisis recovery resource programs.

She began her career in information technology (IT), working in programming and training design at an online training company, before moving into the telecommunications industry. She has worked in various IT roles – including Web design, user experience, business analysis, and project management – before moving into the security/business continuity arena. This diverse background enables her to approach security, risk, business continuity, and disaster recovery with a broad methodology that melds many aspects into a cohesive whole.

Rachelle holds a bachelor's degree in history from the University of North Carolina at Charlotte, and a master's degree in business administration from the University of Phoenix. She is certified as Master Business Continuity Professional (MBCP) through DRI International, as Associate Fellow of Business Continuity International (AFBCI), as Certified Information Security Manager (CISM) through ISACA, and Project Management Professional (PMP) through the Project Management Institute (PMI). Active in multiple business continuity management industry groups, she is vice-chair of the Crisis Management and Business Continuity Council of ASIS International as well as serving on the IT Security Council.

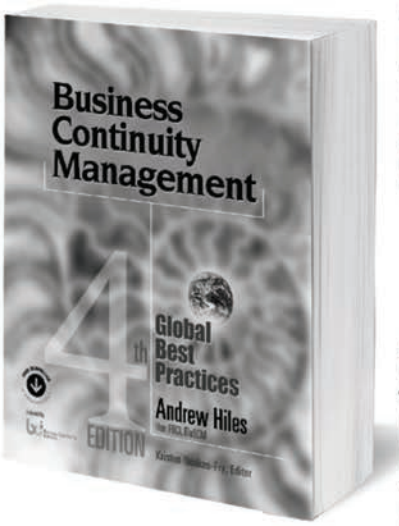
She is the author of *The Manager's Guide to Simple, Strategic, Service-Oriented Business Continuity* (Rothstein Publishing, 2017). In addition, with Brian Allen, Rachelle co-authored *The Manager's Guide to Enterprise Security Risk Management: Essentials of Risk-Based Security* (Rothstein Publishing, 2016).

When the Stakes Are This High, Learn from the Best

Rothstein Publishing Presents 11 New and Current Books/Templates on Business Continuity, Disaster Recovery, and Risk, Crisis, Emergency Management

NEW DIGITAL FORMATS! Get it by the Chapter or by the Book

Make your own eBook – choose only chapters you need from each book, or mix/match chapters from any Rothstein books listed here. See www.rothsteinpublishing .com for details!



The Closest You Can Get to a "Body of Knowledge" for Business Continuity – by an Acclaimed Founder of the Profession

Business Continuity Management:
Global Best Practices, 4th Edition
By *Andrew Hiles, Hon* FBCI, *Elo*SCM

Discover new ideas and inspiration to build world-class Business Continuity Management from this masterwork that distills Hiles' wisdom about what works and why from 30+ years' experience in 60 countries. New 4th Edition is the most international, comprehensive, readable exposition on the subject and now includes:

» New or revised sections: • supply chain risk with contract advice • horizon scanning of new risks • multilateral continuity planning • impact of new IT/Internet technologies • global/national standards, with details on ISO 22301/22313 and NFPA 1600.

» 520-page book + hundreds of pages of downloadable resources, including case studies and examples, questions, forms, checklists, project plans, BIA spreadsheets, sample BC plans, and exercise material. Instructor Resources coming soon.

Andrew Hiles is an internationally renowned practitioner, consultant to major private/public sector organizations worldwide, and trainer of two generations of Business Continuity professionals.

"Andrew Hiles was the main driver in the formation of The Business Continuity Institute and his teachings have provided great leadership to our profession. If you only read one Business Continuity book this year, make sure this is it."

–Lyndon Bird, Technical Director, The Business Continuity Institute

©2015, 520 pages + Downloadable Resources, glossary, index
ISBN 978-1-931332-35-4, paperback 8.5x11 ISBN 978-1-931332-76-7, PDF/eBook
ISBN 978-1-931332-83-5, ePub

Uniquely Two-Books-in-One: Crisis Response AND Crisis Preparedness with Case Studies/Examples of Crisis Leadership Throughout

Blindsided: A Manager's Guide to Crisis Leadership, 2nd Edition
By *Bruce T. Blythe*

Hold-on! This book lands you in the middle of a fast-breaking crisis and uses case studies and examples to demonstrate what a top-notch leader would say and do at every turn. After this eye-opening simulation, the author uses his 30 years of global crisis experience to show you how to develop a highly practical crisis management plan.

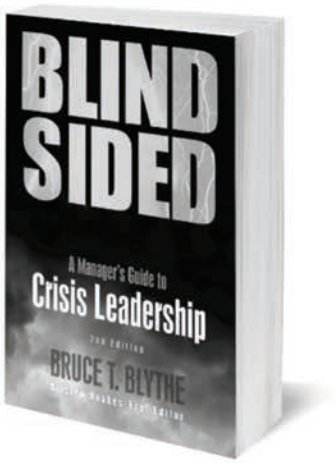
» Chapter action checklists – A Quick Preparedness/Response Guide called by users "worth the price of the book"– plus 9 detailed checklists for major incidents, including accidental deaths, chemical/toxic exposure, explosion/fire, flood.

» Unique guide for addressing victims' families – Dos and don'ts for communicating tragic news with empathy and dignity in person.

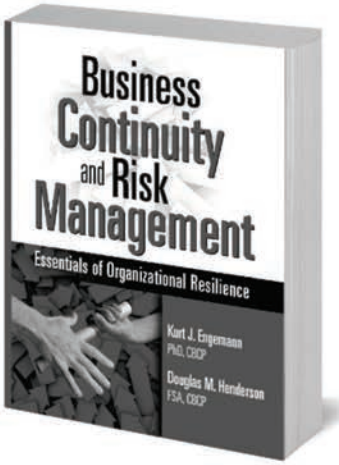
Bruce T. Blythe is a global crisis consultant, executive coach to Fortune 100 managers, owner/chairman of three crisis consulting companies, and renowned speaker.

"Blythe's book is different… a step-by-step guide to process excellence…a veritable encyclopedia of crisis leadership, rich in strategic insights, invaluable for any leader."

— Daniel Diermeier, IBM Distinguished Professor of Regulation and Competitive Practice, Kellogg School of Management, Northwestern University



©2014, 400 pages, glossary, index ISBN 978-1-931332-69-9, paperback 6x9 ISBN 978-1-931332-71-2, PDF/eBook
ISBN 978-1-931332-87-3, ePub



State-of-the-Art Exposition of the "Twin Disciplines"

Business Continuity and Risk Management:
Essentials of Organizational Resilience
By Kurt J. Engemann, PhD, CBCP and Douglas M. Henderson, FSA, CBCP

Business Continuity and Risk Management are now considered twin disciplines and this new text offers a state-of-the-art exposition of the global body of knowledge for their interrelationship.

- 10 chapters cover Business Continuity principles and practices; 3 focus on Information Technology and Emergency Management; and 4 explain Risk Modeling for those wanting statistical underpinnings in Risk Management.
- Extensive Instructor Resources are available for college courses and professional development training, including syllabi, test bank, discussion questions, case studies, and slides.

Authors are a college professor who is also editor-in-chief of the International Journal of Business Continuity and Risk Management, and a Business Continuity consultant with 25+ years of experience.

"It's difficult to write a book that serves both academia and practitioners, but this text provides a firm foundation for novices and a valuable reference for experienced professionals."

– Security Management Magazine

©2012, 370 pages, glossary, index ISBN 978-1-931332-54-5, paperback 8.5 x 11
ISBN 978-1-931332-73-6, PDF/eBook ISBN 978-1-931332-89-7, ePub

Demonstrates That Systematically Managing Individual and Collective Workplace Emotions Is Critical to Risk and Crisis Management

The Cost of Emotions in the Workplace:
The Bottom Line Value of Emotional Continuity Management
By Vali Hawkins Mitchell, PhD, LMHC

Finally – a people management guide that goes way beyond the typical "problem employee" books to help you understand and manage the entire emotional culture of your organization.

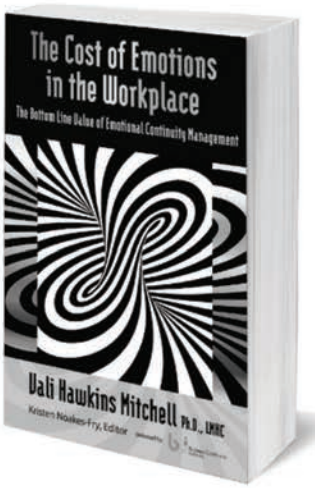
- Introduces the rising field of Emotional Continuity Management (ECM) and provides a tested system to observe, predict, prepare, and write policy to manage the full range of workplace emotions productively – to stop workplace problems before they start.
- Offers tools to quantify bottom-line costs of disruptive emotional incidents, from bad managers, emotional terrorists and office bullies to workplace violence, and includes real-life examples, tips, tools, checklists, forms, and sample plans.

"Dr. Vali" is a Certified Traumatologist, holds a Doctorate in Health Education, and is a highly regarded speaker, consultant, educator, and counselor to victims of major disasters, including 9/11 and Hurricane Katrina.

"You'll look with new eyes at the enormous role played by human emotions in today's business. I endorse it as a guide for the 21st century global workforce."

– James J. Cappola, MD, PhD, Medical Director, Medical Affairs, Harvard Clinical Research Institute

©2013, 300 pages, glossary, index ISBN 978-1-931332-58-3, paperback 6x9 ISBN 978-1-931332-68-2 PDF/eBook
ISBN 978-1-931332-84-2 ePub



Easy Workbook Format Shows Managers New to Business Continuity Planning How to Develop a Basic Plan and Keep It Updated

Business Continuity Planning:
A Step-by-Step Guide with Planning Forms, 3rd Edition
By Ken Fulmer, CBCP

If you've been tasked with developing a basic business continuity plan and aren't sure where to start, this workbook with sample forms, checklists, and plans will walk you step-by-step through the process.

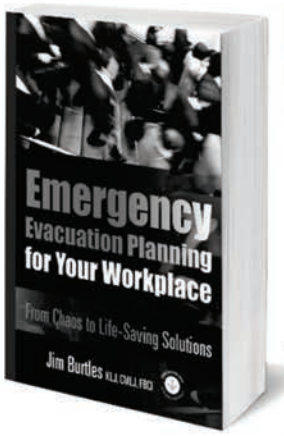
- Extensive, easy to-use downloadable resources include reproducible worksheets, forms, templates, questionnaires, and checklists for various natural disasters and special hazards such as power outages, boiler failures, bomb threats, hazardous material spills, and civil unrest, along with a checklist for vital records storage.
- Straightforward explanations emphasize non-technical aspects of Business Continuity Planning/Disaster Recovery.

Kenneth L. Fulmer, a 30+ year veteran of the computer industry, has published, trained and spoken on business continuity throughout his career.

"This excellent primer sets out a simple, concise, and, most of all, logical roadmap both for developing the justification for a business continuity/disaster recovery program as well as for developing and maintaining the resultant plan."

– Larry Kalmis, FBCI, Project Executive, Virtual Corporation and Chairman, Business Continuity Institute

©2008, 190 pages, + Downloadable Resources, glossary ISBN 978-1931332-21-7, paperback 8.5 x 11
ISBN: 978-1-931332-80-4, PDF/eBook ISBN: 978-1-931332-90-3, ePub



First All-in-One, Practical Resource That Integrates Workplace Emergency Evacuation Planning with Business Continuity

Emergency Evacuation Planning for Your Workplace:
From Chaos to Life-Saving Solutions
By *Jim Burtles*, KLJ, CMLJ, FBCI

Whether you work in facilities management, HR, or emergency, risk and business continuity management, this groundbreaking new book will become your go-to resource for safely evacuating people of all ages and health conditions from workplaces of all kinds.

» Based on 12 years' research into global best practices, it includes a comprehensive package of 600+ pages of book and downloadable resources with tools, templates, case studies, sample plans, forms, checklists, articles, and practical tips.

» Selected by the International Facilities Management Association (IFMA) and endorsed by The Business Continuity Institute (BCI).

Jim Burtles is an internationally acclaimed Business Continuity consultant with 35 years' experience in 24 countries. A founding Fellow of the Business Continuity Institute, he received BCI's Lifetime Achievement Award in 2001.

"Unique, comprehensive, important guide and reference for anyone interested in workplace safety and emergency evacuation planning. Recommended."

– Choice Magazine, Association of College and Research Libraries

©2013, 340 pages + Downloadable Resources, glossary, index ISBN 978-1-931332-56-9, casebound 6x9
ISBN 978-1-931332-67-5, PDF/eBook ISBN: 978-1-931332-85-9, ePub

Selected One of "30 Best Business Books of 2013" by Soundview Executive Book Summaries

Lukaszewski on Crisis Communication: What Your CEO Needs to Know About Reputation Risk and Crisis Management
By *James* E. *Lukaszewski*, ABC, APR, *Fellow* PRSA

America's Crisis Guru draws on four decades of consulting experience confronting crises of every kind to advise you exactly what to do, what to say, when to say it, and when to do it while the whole world is watching. He uniquely emphasizes how to manage the victim-driven nature of crisis.

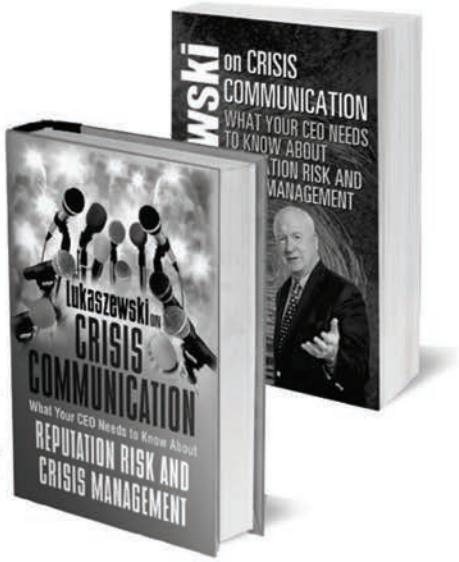
» Tells how to get heard by management and gives step-by-step details for creating a practical crisis communication plan and putting it into action in the real world of victims, media relations, social media, litigation, and activists.

» Packed with case studies/examples, practical tools, charts, checklists, forms, and templates.

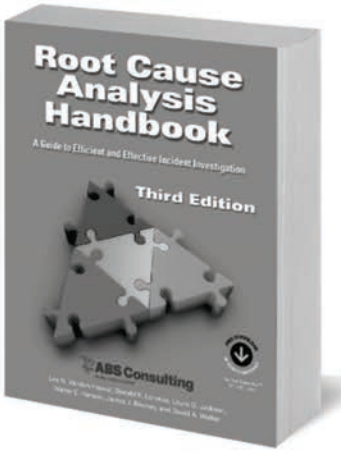
James E. Lukaszewski (loo-ka-SHEV-skee), profiled in Living Legends of American Public Relations, was invited by Penn State University to speak at its 2013 Bronstein Lecture in Ethics and Public Relations and was recognized by the Minnesota Chapter of Public Relations Society of America with the Donald G. Padilla Distinguished Practitioner Award for his role as a PR educator, ethicist, and ambassador.

"Jim is one of the most knowledgeable people on earth about crisis management and his counsel has saved the reputation of many corporations and individuals."

– Jay Rayburn, PhD, Fellow PRSA, Division Director, Advertising/Public Relations, School of Communication, Florida State University



©2013, 400 pages, glossary, index ISBN 978-1-931332-66-8, hardcover 6x9
ISBN 978-1-931332-57-6, paperback 6x9 ISBN 978-1-931332-64-4, PDF/eBook
ISBN 978-1-931332-81-1, ePub



Selected by Risk and Insurance Management Society (RIMS) and American Society for Quality (ASQ)

Root Cause Analysis Handbook:
A Guide to Efficient and Effective Incident Investigation, 3rd Edition
By ABS *Consulting*; *Lee* N. *Vanden Heuvel*, *Donald* K. *Lorenzo*, *Laura* O. *Jackson*, *Walter* E. *Hanson*, *James* J. *Rooney*, *and David* A. *Walker*

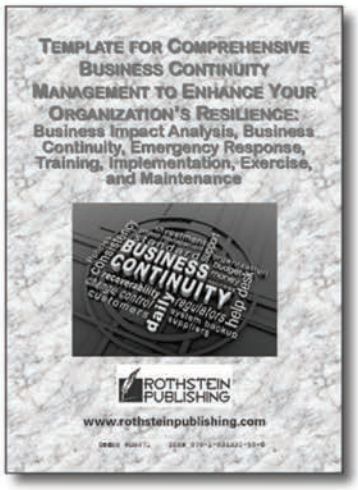
Reach for this bestselling handbook anytime you need to identify and eliminate the root cause of incidents with quality, reliability, production processes, and environmental, health, and safety impacts – and their attendant risks.

» THE most complete, all-in-one package available for root cause analysis, including 600+ pages of book and downloadable resources; color-coded, 17" x 22" Root Cause Map™; and licensed access to extensive online resources.

» Based on a globally successful, proprietary methodology developed by an international consulting firm with 50 years' experience in 35 countries.

A global classic called "in a league of its own" and "the best resource on the subject."

©2008, 300 pages + Downloadable Resources, fold-out map, glossary ISBN 978-1-931332-51-4, paperback 8.5x11
ISBN 978-1-931332-72-9, PDF/eBook, ISBN 978-1-931332-82-8, PDF/eBook



Edit This Powerful Step-by-Step Toolkit to Create/Customize Your Own Business Continuity Plan!

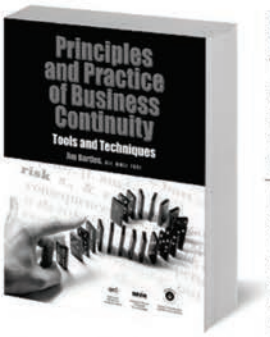
Template for Comprehensive Business Continuity Management:
Business Impact Analysis, Business Continuity, Emergency Response, Training, Implementation, Exercise and Maintenance, 4th Edition
By Douglas M. Henderson, FSA, CBCP

Use this easy-to-follow, editable toolkit to create a professional, comprehensive Business Continuity Plan completely customized to your industry and specific needs -- without straining your time or budget! It also includes specific sub-plans for hurricanes, floods, and pandemics.

- Guides you through a color-coded, editable Microsoft Word format with a complete set of field-tested forms, checklists, tips, sample plans and reports, and reproducible documents for employee distribution – everything you need to prepare every department of your business for an emergency, protect your people, and minimize operational disruptions.
- 1,700+ pages and 50 files help you establish an ongoing Business Continuity System and write, test, and maintain a comprehensive Plan based on best practices and standards.

Douglas M. Henderson, a 25-year consultant in all areas of emergency planning and response, has developed numerous general business continuity, facility-specific, and disaster-specific templates.

©2012, 1,700 editable pages in Microsoft Word ISBN 978-1931332-59-0, CD-ROM

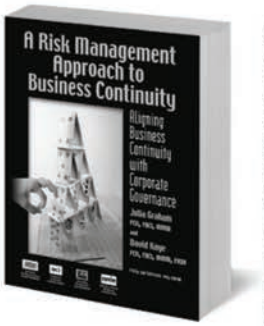


Principles and Practices of Business Continuity:
Tools and Techniques
By Jim Burtles, KLJ, CMLJ, FBCI

Expand your perspectives and expertise by tapping into the vast, global knowledge base of Jim Burtles – recipient of The Business Continuity Institute's Lifetime Achievement Award, an internationally renowned pioneer in Business Continuity Management with 30 years' experience in consulting and teaching in 22 countries, and a counselor during 90 disasters and 200 emergencies worldwide.

- Particularly useful in large multi-location or multinational companies, this book is standards-based, includes global best practices, shows how to develop a comprehensive and rigorous plan, and provides grounding in the principles and practices of Business Continuity Planning. Downloadable Resources include case studies, forms, checklists, and sample plans.

©2007, 320 pages + Downloadable Resources, glossary
ISBN 978-1931332-39-2, paperback 8.5 x 11
ISBN 978-1-931332-79-8, PDF/eBook ISBN 978-1-931332-86-6, ePub



A Risk Management Approach to Business Continuity:
Aligning Business Continuity with Corporate Governance
By Julia Graham, FCII, FBCI, MIRM, Chartered Insurer and David Kaye, FRSA, FCII, FBCI, MIRM, Chartered Insurer

These two global consultants with experience in 50 countries present a practical guide to integrating enterprise-wide risk management, business continuity, and corporate governance. They focus on all the factors that must be considered when developing a comprehensive Business Continuity Plan, especially for multi-location or multinational companies.

©2006, 420 pages, glossary ISBN 978-1-931332-36-1, paperback 8.5 x 11
ISBN 978-1-931332-74-3, PDF/eBook ISBN 978-1-931332-88-0, ePub

ROTHSTEIN PUBLISHING

Rothstein Publishing is your premier source for books and learning materials about Business Resilience – including Risk Management, Crisis Management, Business Continuity, Disaster Recovery, and Emergency Management. Our industry-leading authors provide current, actionable knowledge, solutions, and tools you can put into practice immediately. Founded in 1984 by Philip Jan Rothstein, FBCI, our company remains true to our commitment to prepare you and your organization to protect, preserve, and recover what is most important: your people, facilities, assets, and reputation. Rothstein Publishing is a division of Rothstein Associates Inc., an international management consultancy.

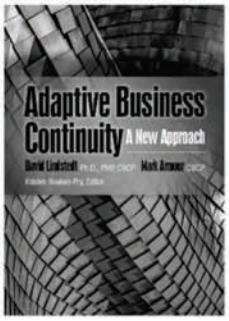
Rothstein publications are distributed worldwide through book retailers and wholesalers and via eBook databases, including EBSCOHost, ebrary/EBL, Books24x7, Slicebooks, IngramSpark, MyiLibrary, VItalSource, and iGroup.

www.rothsteinpublishing.com
info@rothstein.com
203.740.7400
4 Arapaho Rd., Brookfield, CT
06804-3104 USA

facebook.com/RothsteinPublishing
linkedin.com/company/rothstein-associates-inc.
twitter.com/RothsteinPub

New eBooks

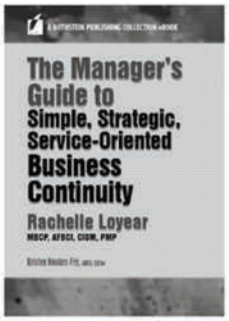
From The Rothstein Publishing eBook Collection



Adaptive Business Continuity: A New Approach

David Lindstedt, Ph.D., PMP, CBCP and and Mark Armour, CBCP
Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) June 2017
ISBN: 978-1-944480-4-0 (EPUB)
ISBN: 978-1-944480-41-7 (PDF)
172 pages

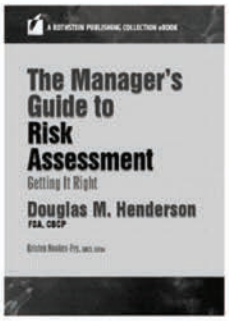
The preparedness planning industry is at a turning point. Circumstances demand that professionals look at business continuity (BC) and its practice in new ways. Adaptive Business Continuity: A New Approach offers an alternative to make your BC program more effective. Adaptive Business Continuity will improve your organization's recovery capabilities.



The Manager's Guide to Simple, Stategic, Service-Oriented Business Continuity

Rachelle Loyear, MBCP, AFBCI, CISM, PMP Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) May 2017
ISBN: 978-1-944480-38-7 (EPUB)
ISBN: 978-1-944480-39-4 (PDF)
145 pages

You have the knowledge and skill to create a workable Business Continuity Management (BCM) program –but too often, your projects are stalled while you attempt to get the right information from the right person. Rachelle Loyear takes you through the practical steps to get your program back on track.



The Manager's Guide to Risk Assessment: Getting It Right

Douglas M. Henderson, FSA, CBCP Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) March 2017
ISBN: 978-1-944480-38-7 (EPUB)
ISBN: 978-1-944480-39-4 (PDF)
114 pages

Risk assessment is required for just about all business plans or decisions. As a responsible manager, you need to consider threats to your organization's resilience. But to determine probability and impact – and reduce your risk – can be a daunting task. Guided by Henderson's The Manager's Guide to Risk Assessment: Getting It Right, you will confidently follow a clearly explained, step-by-step process to conduct a risk assessment.

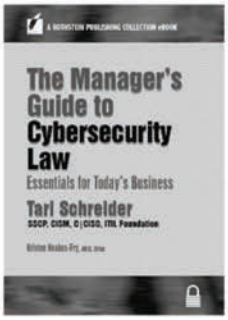
ROTHSTEIN PUBLISHING
A Division of Rothstein Associates Inc.
Brookfield, Connecticut USA
www.rothstein.com

www.facebook.com/RothsteinPublishing
www.linkedin.com/company/rothsteinpublishing
www.twitter.com/rothsteinpub

I

New eBooks

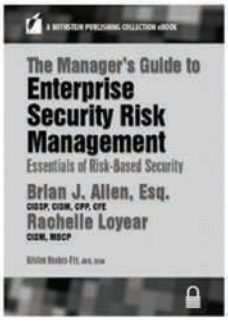
From The Rothstein Publishing eBook Collection



The Manager's Guide to Cybersecurity Law: Essentials for Today's Business

Teri Schreider, SSCP, SISM, C | CISO, ITIL Foundation Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) February 2017
ISBN: 978-1-944480-30-1 (EPUB)
ISBN: 978-1-944480-31-8 (PDF)
168 pages

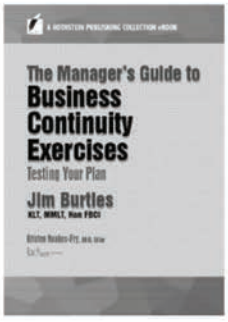
In today's litigious business world, cyber-related matters could land you in court. As a computer security professional, you are protecting your data, but are you protecting your company? While you know industry standards and regulations, you may not be a legal expert, but fortunately, in a few hours of reading rather than months of classroom study you could be.



The Manager's Guide to Enterprise Security Risk Management: Essentials of Risk-Based Security

Brian J. Allen, Esq., CISSP, CISM, CPP, CFE
Rachelle Loyear MBCP, AFBCI, CISM, PMP Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) November 2016
ISBN: 978-1-944480-24-0 (EPUB)
ISBN: 978-1-944480-25-7 (PDF)

Is security management changing so fast that you can't keep up? Perhaps it seems like those traditional "best practices" in security no longer work? One answer might be that you need better best practices!



The Manager's Guide to Business Continuity Exercises: Testing Your Plan

Jim Burtles, KLT, MMLT, Hon FBCI Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) November 2016
ISBN: 978-1-944480-32-5 (EPUB)
ISBN: 978-1-944480-33-2 (PDF)
100 pages

Your challenge is to maintain a good and effective plan in the face of changing circumstances and limited budgets. If your situation is like that in most companies, you really cannot depend on the results of last year's test or exercise of the plan.

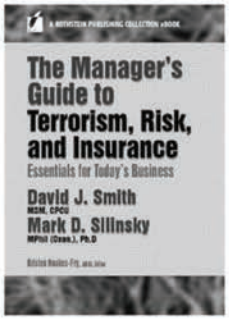
ROTHSTEIN PUBLISHING
A Division of Rothstein Associates Inc.
Brookfield, Connecticut USA
www.rothstein.com

www.facebook.com/RothsteinPublishing
www.linkedin.com/company/rothsteinpublishing
www.twitter.com/rothsteinpub

II

New eBooks

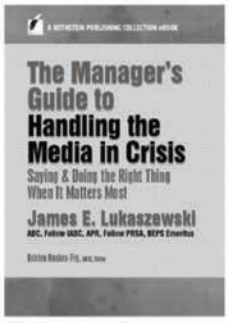
From The Rothstein Publishing eBook Collection



The Manager's Guide to Terrorism, Risk, & Insurance: Essentials for Today's Business

David J. Smith, MSM, CPCU Mark D. Silinsky, MPhol (Oxon.), Ph.D
Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) October 2016
ISBN: 978-1-944480-26-4 (EPUB)
ISBN: 978-1-944480-27-1 (PDF)
120 pages

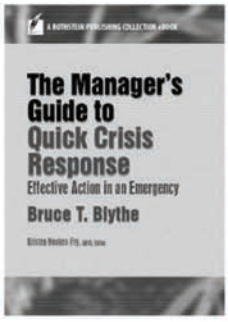
As a manager, you're aware of terrorist acts, are considering the risks, but sense that you need more background. How might terrorism occur?



The Manager's Guide to Handling the Media in a Crisis: Saying & Doing the Right Thing When It Matters Most

James E. Lukaszewski, ABC, Fellow IABC, Fellow PRSA, BEPS Emeritus
Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) September 2016
ISBN: 978-1-944480-28-8 (EPUB)
ISBN: 978-1-944480-29-5 (PDF)
120 pages

Attracting media attention is surprisingly easy – you just want it to be the right kind! If an event causes the phone to ring and TV cameras to appear in your lobby, you need confidence that the people who happen to be at your worksite that day are prepared.



The Manager's Guide to Quick Crisis Response: Effective Action in an Emergency

Bruce T. Blythe Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) August 2016
ISBN: 978-1-944480-23-3 (EPUB)
ISBN: 978-1-944480-22-6 (PDF)
117 pages

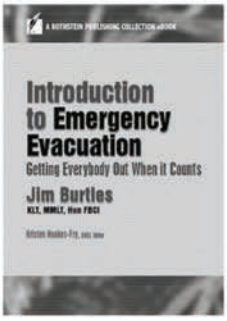
Avoid being "blindsided" by an unexpected emergency or crisis in the workplace – violence, natural disaster, or worse!

ROTHSTEIN PUBLISHING
A Division of Rothstein Associates Inc.
Brookfield, Connecticut USA
www.rothstein.com

www.facebook.com/RothsteinPublishing
www.linkedin.com/company/rothsteinpublishing
www.twitter.com/rothsteinpub

New eBooks

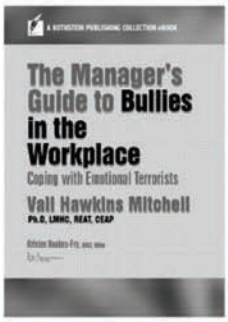
From The Rothstein Publishing eBook Collection



Introduction to Emergency Evacuation: Getting Everybody Out When It Counts

Bruce T. Blythe Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) July 2016 ISBN: 978-1-944480-14-1 (EPUB)
ISBN: 978-1-944480-15-8 (PDF)
120 pages

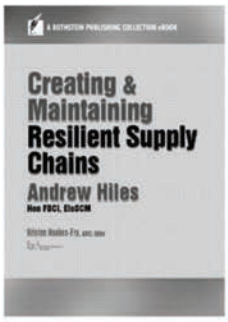
When it's not just a drill, you need to get it right the first time. If an emergency alert sounds, are you ready to take charge and get everyone out of the office, theater, classroom, or store safely?



The Manager's Guide to Bullies in the Workplace: Coping with Emotional Terrorists

Vali Hawkins Mitchell, Ph.D, LMHC, REAT, CEAP Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) July 2016
ISBN: 978-1-944480-12-7 (EPUB)
ISBN: 978-1-944480-13-4 (PDF)
120 pages

As a manager, you can usually handle disruptive employees. But sometimes, their emotional states foster workplace tension, even making them a danger to others.



Creating & Maintaining Resilient Supply Chains

Andrew Hiles, Hon FBCI, EloSCM Kristen Noakes-Fry, ABCI, Editor
(A Rothstein Publishing Collection eBook) July 2016
ISBN: 978-1-944480-07-3 (EPUB)
ISBN: 978-1-944480-08-0 (PDF)
120 pages

Will your supply chain survive the twists and turns of the global economy? Can it deliver mission-critical supplies and services in the face of disaster or other business interruption?

ROTHSTEIN PUBLISHING
A Division of Rothstein Associates Inc.
Brookfield, Connecticut USA
www.rothstein.com

www.facebook.com/RothsteinPublishing
www.linkedin.com/company/rothsteinpublishing
www.twitter.com/rothsteinpub