# Information Risk Management Body of Knowledge

Society of Information Risk Analysts

# Contents

# Chapter 1

# About the Society of Information Risk Analysts

## 1.1 Who We Are

The Society of Information Risk Analysts (SIRA) is a rapidly growing, global non-profit association established to advance the full maturation and mainstream acceptance of Information Risk Management (IRM) as a discipline and profession. SIRA is a professional association which develops, maintains, and disseminates pragmatic, realistic, implementable, evidence-based IRM practices and methodologies.

## 1.2 Contact Us

For more information, please contact the Society of Information Risk Analysts at:

Society of Information Risk Analysts 1023 Delaware Avenue
Mendota Heights, MN 55118
USA
Website: http://www.societyinforisk.org
Contact Form: https://www.societyinforisk.org/contact

# Chapter 2

# Introduction

## 2.1 What Is the Information Risk Management Body of Knowledge?

The Information Risk Management Body of Knowledge (iRMBOKTM) is a standard for the practice of information risk management. The iRMBOKTM Guide describes information risk management tasks and the knowledge required to be effective.

The primary goal of the iRMBOKTM Guide is to define the emerging profession of information risk management. It serves as a baseline that practitioners can agree upon in order to discuss the work they do and to ensure that they have the skills they need to effectively perform the role, and defines the skills and knowledge that people who work with and employee information risk managers should expect a skilled practitioner to demonstrate. It is a framework that describes the information risk management tasks that must be performed in order to understand how an organization may manage its information risks.

This chapter provides an introduction to key concepts in the field of information risk management and describes the structure of the remainder of the iRMBOKTM Guide.

## 2.2 What is Information Risk Management?

Information Risk Management (IRM) is the continuous process of information risk analysis (see Chapter 2: Risk Assessment), information risk treatment (see Chapter 3: Risk Treatment), and information risk communication (see Chapter 4: Communication and Consultation).

## 2.3 Is Information Risk Management a Failed Concept?

While IRM has had its share of critics, probably none has been as vocal as Donn Parker. In a 2006 article in the journal of the Information Systems Security Association, Parker claimed that risk-based security is a "failed concept."1 Parker thinks that there is too much uncertainty and complexity in the data regarding rare incidents to effectively apply the principles of decision theory to information security. Furthermore, even if these obstacles could be overcome, Parker believes "it is too easy for management to accept security risk rather than reducing it by increasing security that is inconvenient and interferes with business."2 Given Parker's well-earned influence in the information security community and the importance of the topic, it's worth considering his objections in detail.

In his 2006 article, Parker proposes that risk-based security "... must be replaced with practical, doable security management with the new objectives of due diligence, compliance consistency, and enablement" (hereafter, "diligence-based security").3 Due diligence is necessary to avoid negligence; compliance to avoid penalties; and enablement to be competitive. According to Parker, "Reduction of security risk then becomes serendipitous." In his more recent writings, Parker has avoided any implications that his diligence method attempts to meet or is related to the legal concept of due diligence, by referring to diligence only.

Here we need to be careful to distinguish three options regarding the foundation for information security management:

- Information security management based upon diligence-based security only.
- Information security management based upon risk-based security only.
- Information security management based upon both risk- and diligence-based security.

Parker endorses (I), whereas I shall argue for (III). What is striking about Parker's article is that he writes as if the only options were (I) and (II), but that is a false dichotomy. It seems to me that diligence- and risk-based security are complementary, in four ways.

First, compliance often requires risk-based security. As Parker himself now admits, some laws require information security risk analysis (ISRA). In the U.S., such laws include the Federal Trade Commission Act ("FTC Act"),5 Gramm-Leach-Bliley Act (GLBA),6 the Federal Information Security Management Act of 2002 (FISMA),7 etc. Outside of the U.S., such laws include the EU Data Protection Directive8 and Japan's Personal Information Protection Act.9 Furthermore, contractual obligations can require an organization to perform a formal risk assessment. For example, many organizations are contractually obligated to comply with the Payment Card Industry (PCI) Security Standards Council's

Data Security Standard (DSS), which in turn requires an annual risk analysis (RA).10 Along the same lines, any organizations subject to any of the U.S. state laws mandating PCI DSS compliance11 arguably have a duty to perform an RA.

Second, business enablement should properly be taken into account in an effective RA, as failing to enable the business amounts to a failure to achieve business objectives, which is broadly equivalent to risk.12 Third, new and emerging security threats are especially problematic if one eschews a risk-based approach to security. When a new threat is discovered, laws are unlikely to mandate specific security controls to deal with that threat. Moreover, due diligence is unlikely to be helpful either, since there probably will not be any de facto industry standard for mitigating that threat. For example, laptop encryption is surely part of the standard of care today, but it was not five years ago.13 Additionally, compliance is often the lowest common denominator that protects entities outside of an organization (e.g., consumers, government, payment card brands) more than the organization itself. Compliance is rarely an efficient way of allocating resources, since compliance requirements are rarely (if ever) designed with a specific organization's nuances in mind.

Fourth, there are often multiple options that can be used to avoid negligence, achieve legal compliance, and enable the business. Organizations have limited resources to invest in information security. Sometimes the resources required just to achieve compliance, due diligence, and enablement exceed the resources that are available. Lawmakers and other organizations need a decision making method for selecting one of those options. The methods of decision theory, including risk analysis, are empirically well supported. The diligence-based method is not.

Furthermore, while Parker has modified his position by removing an appeal to the legal concept of due diligence, that does not deny the fact due diligence to avoid negligence itself requires a risk- based approach. Let us define due diligence as the prudent person's fulfillment of the duty to use reasonable care; negligence is the failure to do so. In this context, "reasonable care" means "such care as what a reasonable prudent and careful person would use under similar circumstances."

In United States v. Carroll Towing Co, Judge Learned Hand determined that a party has a duty to take adequate measures to prevent harm if the cost (B) of taking adequate measures to prevent harm is less than the monetary loss (L) multiplied by the probability (P) of its occurring, expressed by the equation "$B < PL$." Thus, the due diligence needed to determine a party's duty of care requires a cost- benefit analysis that weighs the risk ($P \times L$) against the cost (B) to mitigate that risk.

Moreover, as explained by U.S. Supreme Court Justice Holmes in Texas & P.R. v Behymer, "[w]hat usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it

is usually complied with or not."17 There is strong evidence that risk-based security is the standard. First, several high-profile U.S. organizations have publicly endorsed security risk management, including the Government Accountability Office,18 the Federal Trade Commission,19 the U.S. Marine Corps,20 the U.S. Air Force,21 and Microsoft.22 Second, a number of professional societies and standards bodies advocate security risk management, including the Information Systems Security Association (ISSA),23 the Information Systems Audit and Control Association (ISACA),24 the American Society for Industrial Security (ASIS),25 the Institute of Internal Auditors (IIA),26 Standards Australia and Standards New Zealand,27 the British Standards Institute,28 the U.S. National Institute of Standards and Technology,29 and, most notably, the International Organization for Standardization.

As I read him, Parker's critique of risk-based security consists of eight supporting arguments. Those arguments may be divided into three categories: theoretical, empirical, and practical. Let us examine each of his supporting arguments in turn.

### 2.3.1 Theoretical Arguments against Risk-Based Information Security

Let's begin by considering Parker's arguments against the possibility of actually doing risk-based security in the real world.

#### 2.3.1.1 First Supporting Argument: Uncertainties Involved in ISRA

Here is Parker:

> The frequencies and impacts of future incidents are under the control of unknown and often irrational enemies with unknown skills, knowledge, resources, authority, motives, and objectives from unknown locations at unknown future times attacking known but untreated >vulnerabilities and vulnerabilities that are known to the attackers but unknown to the defenders (a constant problem in our >technologically complex environments).

This objection to risk-based security is multiply flawed.

First, many of the variables listed by Parker are simply not relevant to assessing the probability of an attack. One does not need to know the identity of an attacker, much less his "skills, knowledge, resources, authority, motives and objectives" (SKRAMO), in order to estimate the probability of an attack. There is no doubt that we often lack knowledge about the SKRAMO of our attackers, but that doesn't mean we cannot calculate the probability of an attack.

Suppose we have historical data about the frequency of occurrence a particular type of security threat spanning multiple years, across multiple organizations of varying size, geographical location, and so forth. For example, let the threat be workplace violence, a threat that involves "irrational, unknown humans." Based on the historical data just mentioned, one can infer a statistical generalization about the frequency of the workplace violence threat overall. One can also make more specific generalizations about various subsets of the overall workplace violence threat. For example, one can make statistical generalizations about the rate of incidents of workplace violence in organizations that recently went through a round of layoffs, in individuals who were subject to one or more negative personnel actions, and so forth.

My claim is that, as a security professional, I can use that statistical data in a quantitative RA of the workplace violence threat for my company. Yes, there are differences between my company and the other organizations for which we have statistical data about incidents of workplace violence. But the mere existence of such differences doesn't automatically invalidate inductively correct or statistically valid inferences about the level of risk for my company, given what we know about the rate of occurrence of workplace violence in other companies. In order for such inferences to be inductive incorrect or statistically invalid, one would have to show that the differences between my company and other companies are probabilistically relevant.

Suppose Microsoft announces tomorrow the existence of a previously unknown security vulnerability in one of their software products. There won't be any historical data tomorrow regarding the rate of occurrence of attempted exploits of that vulnerability. There won't be any historical data tomorrow regarding our enemies and whether they are planning on exploiting that vulnerability. Despite that lack of data, however, we can still make accurate calculations of the level of risk, based upon what we know about past security vulnerabilities and past enemy attacks.

Second, even in those situations where historical data about the statistical frequency of a specific threat is unavailable, historical data is often available for some larger class of events for which the specific threat is a member. Every time a new vulnerability is announced in a given piece of software, by definition there will be no historical data about that vulnerability. Yet we have a large amount of statistical data about information security vulnerabilities in general. We also have a wealth of historical information about vulnerabilities affecting specific types of software. For example, the next time a new vulnerability in the Apache web server software is announced, we won't have any statistical data regarding the frequency of exploits of that specific vulnerability, but we will have data about the frequency of past Apache vulnerabilities for which exploit code is publicly available. That latter data is relevant to determining the probability that exploit code will be made publicly available for the new vulnerability.

A similar point applies to the worry about threats stemming from the acts of individuals (as opposed to "acts of nature"). While we may not have any

historical data about the probability of a specific enemy committing attack Y, we do have statistical data about attacks in general, specific types of attacks, and attacks against specific organizations. To be sure, the more specific the reference class, the more confidence we will have in our probability values. Just because our reference class is not identical to the event in question, however, it does not follow that we cannot have a reasonable or even high degree of confidence in our probability values. The fact that we cannot know something with certainty (i.e., probability = 100%) does not prevent us from knowing it with a high degree of probability (i.e., probability > 50%).

Parker also introduces the following related objection:

> In addition, when enemies fail in attacking one possible vulnerability, they often attempt attacks on other vulnerabilities to >accomplish their goals. Therefore, risks may be related in unknown complex ways so that reducing one risk may increase or decrease >other risks. This alone precludes the effective use of risk assessment methods.32

Parker is certainly correct that if an initial attempt to exploit a vulnerability fails, many attackers will try other attacks in order to accomplish their goals. It does not follow, however, that this fact "alone precludes the effective use of risk assessment methods" (emphasis mine). This is an incredibly strong claim that requires a supporting argument from Parker, but such an argument is not provided in his article.

In sum, far from disqualifying the use of RA, our uncertainty about attackers provides a strong reason for using probabilistic, risk-based methods. As Doug Hubbard writes, "We use probabilistic methods because we lack perfect data, not in spite of lacking it. If we had perfect data, probabilities would not be required."33 Furthermore, "It is a fallacy that when a variable is highly uncertain, we need a lot of data to reduce the uncertainty. The fact is that when there is a lot of uncertainty, less data is needed to yield a large reduction in uncertainty."

#### 2.3.1.2 Second Supporting Argument: Complex, Unknowable Relationships between Risks and Security Efforts

Parker's next argument claims that that the relationships between risks and security efforts are complex and often not completely knowable: