PRAGMATIC Security Metrics

Applying Metametrics to Information Security

W. Krag Brotby and Gary Hinson

Preface by M. E. Kabay, PhD, CISSP-ISSMP
Chapter 2

Why Measure Information Security?

Every CSO should have half a dozen dials to watch on a regular basis. These indicators could be “survival metrics,” the hot buttons on a dashboard you are expected to address that monitor the wellness of your organization or an issue of particular concern to management.

George K. Campbell (2006)

Given that so many organizations evidently cope without much in the way of information security metrics, it seems reasonable to explore the reasons why we believe measuring information security is worthwhile although not absolutely essential.
Good practices may, in fact, suffice in some circumstances, but a one-size-fits-all approach will never be optimal and inevitably will result in overprotection of some assets and under-protection of others.

From our experience, we believe there is a genuine and increasingly urgent need for viable metrics in information security. While, to date, the profession has generally muddled through with almost no rational, sound, and defensible security measurements, the situation is simply not sustainable over the long term. We are fast approaching and, in some cases, already exceeding the limits of the information security manager’s gut feeling, qualifications, and experience, coupled with the use of ill-defined and generic good or so-called best practices, as a basis for extremely important security and risk management decisions. While not so common these days, there are still those who contend that as long as you implement best practices, you don’t need extensive metrics. However, best practices are an inadequate substitute for genuine knowledge. What may be best in one organization may be too costly and excessive in another or, in some cases, wholly inadequate. Without metrics, how would you ever know?*

Improving information security is becoming ever harder given that we have already, to a fair degree, harvested the low-hanging fruit. And, unfortunately, as our rate of improvement declines, there are clear signs that organized criminals, hackers, saboteurs, industrial spies, fraudsters, malware authors, and terrorists are gaining the upper hand, perceptibly raising the stakes. It is not far off the mark to suggest that the profession is in, or is fast approaching, a crisis of confidence. We’re winning occasional battles but losing the war. When experienced security professionals turn from being just ordinarily pessimistic and risk-averse to jaundiced and cynical and retiring or leaving the profession for less stressful occupations, is it any wonder that business managers and stakeholders begin to lose faith in our abilities?

The bulk of this chapter consists of a string of rhetorical questions or issues that raise their ugly heads in some form in most organizations at some point. Count yourself lucky if you haven’t been asked them yet: it’s just a matter of time.

The points that follow would form the basis on which one might justify the investment needed to specify, design, and use an *information security measurement system*, leading to (we hope) a convincing business case for such a system and, potentially, justifications supporting at least the initial suite of security metrics that populate it. Don’t fret: we will discuss the measurement system, the selection of metrics, and all that in later chapters, but let’s start by considering the fundamental requirement for security metrics.

* We hear, “You can’t manage what you can’t measure” quite often. It’s an old saw. The phrase has a ring of truth to it, but actually we do manage unmeasured things all the time, just not particularly well! We contend that a lot of information security managers have been struggling to manage information security with inadequate measures because they had no alternative—until now.
2.1 To Answer Awkward Management Questions

Your organization is not ready for a metrics program if you do not have a clear, formal understanding of your goals; strategic plans; policies, procedures and guidelines; existing, repeatable processes; and open lines of communication with stakeholders.

Samuel A. Merrell

We opened this book with an imaginary internal memo from the CEO to the information security manager, urgently seeking answers to a bunch of questions that turn out to be rather difficult to answer without the ability to measure various aspects of information security. Let’s now explore some more of those awkward questions:

- **Are we secure enough?** Realistic managers should not actually anticipate the organization being perfectly secure and free of all information security incidents, but it is perfectly reasonable for them to seek assurance that avoidable incidents are (mostly) being avoided while any incidents that do occur cause minimal (ideally negligible) or, at least, manageable impacts. Management also wants to be reasonably confident that the information security measures in place are adequate to address the risks. This is a rational—if naive—question for management to pose, yet it is fiendishly difficult to answer without metrics and, to be frank, still tricky to address even with solid metrics. “Are we secure enough?” is arguably the $6 million question, the elephant in the security metrics room.

- **Are we more or less secure than our peers?** Assuming that our organization is, in fact, comparable with industry peers, we don’t want to overspend or underspend on security, so they could be our benchmark. On the other
hand, appearing to be more secure than them may actually be worthwhile, in terms of both the brand value of security and in deterring potential adversaries, encouraging them to divert their attentions to our competitors (and, by the way, the same point applies in reverse: are our peers truly as secure as they appear to be?). The fact is that the perception of security can be nearly as important as the reality. And if we are in a highly regulated industry subject to punitive sanctions, we clearly don’t want to be at the bottom of the heap presenting a prime target for enforcement actions.

- **Which are our strongest and weakest security points?** What are the things we can and should build upon, respectively? Note that there is more to this than just identifying and addressing information security vulnerabilities. Security strengths and capabilities (such as multifactor authentication) can be leveraged to develop new lines of business that would be reckless for our less capable competitors.

- **What are our biggest security threats or concerns?** This is important both in the present context and in the future, for instance, in connection with new business ventures or relationships, product lines, processes, or systems. Depending on the business sector, these threats can differ greatly in terms of potential impact.

- **Are we spending (investing) too much or too little on information security, or do we have it about right?** Are we investing wisely, spending on the things that will benefit the organization the most and support its strategic goals? Would additional investment in certain areas be cost-effective (e.g., enabling business processes or opportunities that would otherwise be too risky), and, if so, which are the preferred security investment options? When times are hard, in which areas of information security would it be safest to make cutbacks, and, conversely, which ones would we be foolish or even reckless to cut? Security metrics can be used both to demonstrate the value of information security and justify the ongoing investment, two activities that challenge even the most seasoned and battle-scarred information security veterans.

- **Are our security resources allocated optimally?** Do we implement the security technologies du jour simply because others do? Have we truly considered the return on investment for major security investments, such as IDS/IPS? Are we perhaps missing out on opportunities to implement more cost-effective information security controls, such as security awareness and training, or generally accepted standards of good security practice?

- **Have we properly and adequately treated all reasonably foreseeable information security risks?** Are any nasty surprises lurking around the corner? This is a complex question because definitions of “properly and adequately” may be called into question if there are incidents, while “reasonably foreseeable” gives management plenty of wiggle room to deny its accountability for poor management decisions.
Why Measure Information Security?

- Can we handle compromises, breaches, and other information security incidents effectively and efficiently? What about more serious ones, including outright disasters? Are we sufficiently well prepared to cope with unknown difficult situations that may arise, or are we operating on a knife edge where one more serious incidents may tip us over?

- Are we (sufficiently) compliant? Are we fully compliant with the obligations that really matter? While we must comply fully with many of our security obligations, on some, we may wish to defer full compliance until a more appropriate time, and for a few, we may make a rational management decision that it will be less costly to accept the consequences of noncompliance than to implement security controls purely for the sake of compliance; in other words, full compliance may not be in the organization’s best interests. Will the auditors, regulators, and business partners/customers give us a clean bill of health if they review our information security and related matters, such as risk management, governance, and compliance?

- Are we best in class? Are we perhaps overdoing it, or are we lagging the field in information security? Which parts of our information security management system are performing relatively weakly, and which are leading the way? Would we be able to defend our position on information security to stakeholders, the stock markets, and the news media if probed or if a serious security incident occurred? Can we genuinely claim to have done everything we could to secure customer data? As a number of court cases involving a bank’s responsibility for protecting customers’ accounts have demonstrated, this is far from a straightforward issue. Legal decisions have differed significantly with nearly identical cases being decided both for and against the banks. Having credible metrics demonstrating not only that the organization has a decent set of security controls in place, but that management takes information security seriously enough to invest and take an interest in the measures, would, we feel, bolster their case. It will not inspire comfort, confidence, and credibility if the CEO or CIO gets all flustered on the witness stand when asked basic questions, such as “When was the last time this happened?” or “How many times has this kind of incident happened before, exactly?”

In this context, we are amused to note that fully 43% of the ~10,000 respondents to the Global State of Information Security 2012 survey consider they are not merely “strategists” but “front-runners” with respect to their approach toward information security (Figure 2.1).

* There’s a sting in the tail here, however. Management has no excuse for failing to act on serious security issues that were clearly evident from the metrics. We’ll return to that depressing thought in Chapter 10.

† See PwC (2011).
And we can’t help but wonder if they are all using information security metrics to the best effect.

2.2 To Improve Information Security, Systematically

Our information security controls are never going to be perfect; we know that. Worse still, they seldom remain good enough for long in practice because, despite our efforts, the risks are constantly changing around us, and controls inevitably degrade over time. And it seems that as quickly as we plug the holes in the dam, others appear. We therefore need to update and adapt the security controls to catch up with current risks, at the very least, if not to get ahead of the game where opportunities present themselves. Security improvement is vital because nobody would seriously accept further declining standards, and even stasis is patently not good enough, given the enormous costs of major security incidents that hit the news media every few months.*

It could be argued that we have gotten where we are today mostly through a process of trial and error, hit or miss. Most of us try to learn from our own mistakes, and the best of us also learn from the mistakes made by others. Learning the lessons and making changes to prevent recurrence is perhaps the most important part of incident management, yet it’s hard to do this if the corporate culture is generally to sweep things under the carpet wherever possible in order to save face and avoid further embarrassment. If we don’t even track and record incidents properly and can barely guess at which incidents are costing us the most each month or year, how can we determine which changes are truly worth making? With a system in place to capture the numbers and adopt the learning points from security incidents,

* You could say we are running to stay still.
we can at least recover some of the lost value and move ahead instead of merely keeping pace or falling behind. Capturing, analyzing, and using statistics and other information concerning security incidents is just one example of how we can make the process of improving security more systematic.

Other systematic improvements include the following:

- **Driving strategic alignment** between the business and information security, which means identifying and dealing rationally with any discrepancies or, even better, avoiding such discrepancies by integrating strategic information security planning activities with other strategic business planning in areas such as governance, risk management, and compliance, of course, plus business development and new product development.

- **Improving risk management.** Uncertainty is the core issue in risks in all forms. We already know we need to deal with commonplace security incidents, and we would be negligent if we failed to do so adequately. However, we still have choices over how best to deal with them (e.g., balancing deterrent, preventive, detective, and corrective controls and minimizing threats, vulnerabilities, or impacts). With less common incidents, we also face additional decisions, such as which ones we need to address and when we need to address them or whether to simply deal with them as they occur. We need to address information security risks in a rational way (dealing with uncertainty through probability and assurance), for instance, by developing suitable policies, standards, procedures, or guidelines showing how we intend to treat the risks in a way that meets both security and business objectives. We need to evaluate the threats, vulnerabilities, and impacts, which means we really need to measure them. In other words, we need threat metrics, vulnerability metrics, and impact metrics. These will encourage management to dig beneath bland risk scores and heat maps to identify opportunities to address the threats, vulnerabilities, and impacts through security controls and other forms of risk treatment.

- **Improving security management**—understanding information security, risk management, and related fields and appreciating the dependencies and interrelationships. Determining whether the changes we are making or have already made are actually improving things, for example, developing cost–benefit analysis of security investments beyond being merely a way to justify the business case but elaborating on the projected benefits to generate a set of metrics that will allow us to milk every last ounce of value from the investment. Making security changes where necessary, knowing that changes are often interrelated (as a crude example, if we transfer skilled security professionals to particular tasks, whatever tasks they leave behind are probably going to suffer—more on resource management below).

- **Systematically improving security controls.** “Systematically” is an important point. Without decent metrics, security management is rather hit or miss.
We are forced into making changes based on gut feeling and instinct without really knowing whether those changes are needed, nor whether things are even going in the right direction. We need to be finding and plugging security gaps before they are exploited, ideally doing so in a risk-aligned manner, that is, dealing first with the most severe and pressing risks as a priority. When resources are limited, we should be able to rein in nonessential spending in order to focus on the parts that really matter, implying that we have more than a vague notion of which bits we can afford to let drift for now.

- **Optimizing the value** of information security. This is a key issue for information security professionals because the department’s budget depends on persuading management of the need to invest in information security rather than in other areas; it is equally important for management to know that they are, in fact, getting better returns from security investments than from other options.

- **Improving resource management**, for example, prioritizing information security work (such as security testing of new/changed application systems) relative to other business activities (such as nonsecurity testing and implementation of those systems) and allocating resources effectively, for example, investing in the security infrastructure, being a suite of controls that have multiple applications and so forming the foundation of a solid security structure, but, at the same time, ensuring the infrastructure is sufficiently flexible and suitable for current and future needs.

- **For performance measurement**, allowing us to direct resources and improvement efforts toward the weakest areas of security or, rather, to those that have the greatest potential for improvement.

- **Raising security awareness** in a general sense, for example, using data concerning the frequency of malicious packets received from the Internet to illustrate and reinforce awareness and training messages about the importance of network security.

- **Planning** and sequencing security improvements sensibly, for example, designing and implementing enterprise-wide security architectures comprising common interoperable controls used by many systems.

- **Predicting security risks** based on rational analysis of the prior and current information security situation rather than pure guesswork. The closer we approach certainty, the easier it is to convince management to spend on security and the more confident we are that we are allocating finite resources to the most appropriate areas.

### 2.3 For Strategic, Tactical, and Operational Reasons

We will explore this aspect further in Chapters 4 and 12.
Why Measure Information Security?

- **Supporting strategic (long-term) security decisions.** What does the CIO or information security manager really need to know to guide and direct the information security management function confidently in the years ahead? Where are we or, rather, where should we be heading and what are our objectives in order to mature our information security management system and support or enable strategic business initiatives? If information security management were a cruise ship, typical strategic issues would be deciding which global markets to pursue, what strategic partnerships to develop, how many other ships there should be in the fleet, and what their respective roles are. What are the ports of call, what regulations must be dealt with, who are the customers, and what are the risks that must be managed? In other words, where is the organization headed, what are the strategic objectives, and how do we get there?

- **Supporting tactical (day-to-day) security management decisions.** What does the information security manager need to know to plan the department’s projects during the weeks and months ahead? Are we heading in the right direction to achieve our strategic objectives? Do we have enough fuel (resources) left to get there? What are the most pressing ship-management issues, and what more do we need to do to prevent everything else becoming urgent too? Many, but not all, technology decisions are tactical in nature. Information security risks should be taken into account when considering the adoption of new technologies, for example, but what does that actually mean in practice? A comparative measure of the information security aspects of different technologies would help management make vital decisions, provided it was both credible and available to them, even if, unfortunately, information security is not the ultimate deciding factor! By analogy: where are we headed on the present voyage, what route should we follow, and how are we getting there? Do we have enough fuel?

- **Supporting operational (hour-by-hour) security decisions.** What information are the information security officers, architects, analysts, and administrators most likely to need when deciding which security tasks to tackle next in the hours and days ahead and how to tackle them? Which way and how far should we turn the ship’s rudder? How is the engine doing? Is the fuel pump working correctly?

Leading organizations give considerable attention to base lining, benchmarking, and the collection and analysis of IT performance information. They use a variety of data collection and analysis tools and methods that serve to keep them informed but without imposing unnecessary reporting burdens. They also periodically review the appropriateness of their current measures.

GAO (1998)
2.4 For Compliance and Assurance Purposes

For compliance purposes, including legal, regulatory, and contractual obligations, plus certification against information security good practice standards, such as ISO27k and policies mandated by management. Detailed individual information security measures can be used to disclose the extent of compliance or noncompliance to specific information security requirements, and aggregate metrics can point out whether the organization faces problematic noncompliance with certain laws, regulations, contracts, standards, or policies.

For due diligence (finding out what we ought to be doing) and due care (actually doing the things we know we ought to do). In most jurisdictions, due care is a legal standard to do those things that a person of similar competence would do in a similar situation. In the information security context, due diligence involves management making the effort to discover whether the organization faces unacceptable information security risks despite the presence of a variety of information security controls. Some organizations have the role of information asset owners,* meaning managers who are held personally accountable by their peers for the protection of certain information systems, processes, and information. In order to fulfill their obligations, information asset owners are expected to ensure that security risks affecting their information assets are assessed and monitored, decide how to treat the risks (i.e., accept them, avoid them, transfer them to others, or mitigate them through controls), and ensure that the risks are duly treated. Information security metrics derived from risk analysis can inform information asset owners about the significance of the risks. Metrics relating to the coverage and effectiveness of the information security controls and other forms of risk treatment are obviously useful for due care: if the metrics reveal that the controls are inadequate or missing, something needs to be done. Ideal PRAGMATIC metrics take that a stage further by indicating more specifically what ought to be done in advance of any incidents.

For assurance and reassurance purposes. Providing credible evidence should help convince auditors, reviewers, assessors, and, ultimately, stakeholders that our information security and risk management practices are sound. While we can’t ever be 100% secure, wouldn’t it be good for information security, risk management, and IT audit professionals to be able to reassure management and other stakeholders that they are secure enough? Having the numbers to

* Information asset owners feature a number of times in this book. We make no bones about it: We feel the concept is an excellent, pragmatic means of holding individuals accountable for protecting valuable corporate information assets assigned to them, which, in turn, forces them to take their information security responsibilities seriously for once.
back up those claims adds credibility and confidence to the declarations and, by the way, reduces stress levels in those making them.

For *accountability* in situations where an authority, customer, business partner, head office, owner, or other stakeholder has a direct interest in the organization’s information security controls. It is neither feasible nor sensible, economically and practically speaking, for all the stakeholders to review or audit an organization’s information security arrangements individually. To a certain extent, they can rely on security certification and accreditation schemes (such as ISO/IEC 27001:2005 and PCIDSS) and formal management statements regarding the organization’s security status, but how much better would both approaches be if they were accompanied by meaningful, well-designed, and, most of all, credible information security metrics?

### 2.5 To Fill the Vacuum Caused by Our Inability to Measure Security

If we had no information security metrics and did not measure information security at all, here are just a few of the problems we would face:

- Management and other stakeholders would probably assume that information security is not important or at least not as important as the things that are measured and reported routinely—like finance, for example. They may say business runs on numbers, but what they really mean is that business runs on dollar figures. If we literally can’t put a figure on the value of information security, we’re on a losing streak already.
- The information security function would only come to management’s attention after a major security incident in a distinctly negative light. There would be little management appreciation of the role information security plays in avoiding, preventing, and mitigating many other security incidents or in enabling a range of business activities that would otherwise be too dangerous to undertake.
- Investing in information security would be pure guesswork with no idea whether we are investing enough in the right things. There is a good chance we would not be investing in security at all, except perhaps for compliance with certain obligations, and, even then, it would probably be viewed as an expense, not an investment.
- A strong information security function might be able to use FUD (fear, uncertainty, and doubt) to obtain a budget for whatever it felt like doing with no way for management to determine whether those things were appropriate nor whether they were achieved.
The security manager would only be able to determine when risk was unacceptable by his or her termination.

If anyone asks us whether we are secure, we would be unable to answer truthfully or provide evidence to back up our assertions.

Information security incidents would come as a complete surprise or shock out of the blue.

There would be no way to compare the organization’s information security arrangements against requirements, standards, or comparable organizations (benchmarking).

It is noteworthy that in a PWC survey (PWC 2011), a quarter—yes, a quarter—of the ~13,000 global security and IT managers surveyed reported that they didn’t even know if they had any security incidents in the past year. A third reported not knowing what kind of security events they had or the causes. Given this lamentable lack of the most basic knowledge, we have to wonder what their security budgets are based on.

2.6 To Support the Information Security Manager

Having valid metrics enables business managers to make rational, sensible, and, for that matter, defensible decisions about information security. No longer must they rely entirely on advice from information security professionals or generic good practice standards, laws, and regulations. This has two important consequences for the information security manager:

1. Decisions about whether certain information security risks are acceptable or need to be treated in some way should, by rights, be made by the owners or custodians of the information assets that would be harmed, devalued, or destroyed if the risks materialized, causing security incidents. The information security manager has heretofore been forced to make such decisions on behalf of the information asset owners, either by laying down the rules or by strongly advising management to take a certain course of action. With suitable metrics concerning risks and controls, information asset owners can decide things for themselves. This aligns directly with the governance practice of holding information asset owners personally accountable for protecting and exploiting their information assets.

2. The information security manager can relax a bit. Yes, that is important! Managing information security is a stressful, thankless task without the added pressure of being responsible for security without, in many cases, having the resources to make things adequately secure.
2.7 For Profit!

The ultimate aim of information security is, in a word, sustainability and is achieved through the following:

- **Cutting losses:** minimize information security incidents in number or severity/impact in a cost-effective manner.
- **Increasing assurance:** give management and other stakeholders a degree of confidence that information security risks are in hand and there are no unacceptable risks that exceed the organization’s risk appetite.
- **Supporting the business:** enable the organization to conduct business activities that would otherwise be too risky.
- **Enabling rational decisions:** for example, choosing between alternative or complementary forms of risk management (such as incident prevention, incident response, resilience, recovery, and insurance), ideally adopting the most cost-effective approach, or when to take action of some sort, such as adding countermeasures, changing course, or increasing capabilities.

Information security metrics allow us to implement better, more cost-effective security controls that align with and support the organization’s business objectives. Furthermore, designing, developing, maturing, and using the *information security measurement system* present opportunities for management to review and reconsider how security impacts those objectives—to some extent, it’s chicken and egg: effective security metrics are derived from sound security objectives effectively supporting the business and *vice versa*.

Metrics offer a rational basis on which to challenge the accepted wisdom in information security, for example, using measurements and analysis to prove that certain traditional controls (such as regular password changes) are not only wasteful but may be counterproductive, even harming security. That exemplifies a situation in which metrics may enable us to remove, modify, or moderate security controls: security is not necessarily a matter of continually increasing controls!

**Tip:** Imagine being in a position to suggest to management that certain security controls might safely be retired and the security budget reduced and having the data to substantiate your claim. Once management overcomes the shock, it’s likely your credibility would gain a few notches. Metrics could do that for you. They can also help you and your management allocate what resources you can obtain to best effect.
2.8 For Various Other Reasons

You, your management, or other stakeholders may well have excellent reasons for wanting to measure your information security beyond those we have mentioned so far. Take the U.S. government as an example: it spends a fortune in taxpayers’ money through numerous government agencies and is bound to be held accountable in various ways if those agencies fail to perform, for example, if they experience serious information security or privacy incidents. If the incidents were clearly avoidable, questions will surely be asked. U.S. taxpayers and the government are perfectly justified in seeking assurance that the agencies are, in fact, paying sufficient attention to their security and privacy requirements and spending their budgets wisely. The situation is probably much the same for other governments and, in fact, other federal or group structures where security budgets are centrally allocated and monitored or, more importantly, where the ultimate accountability for information security failures ends up…but naturally the details vary between organizations.

In the United States, the Dodd-Frank Wall Street Reform and Consumer Protection Act resulting from the financial meltdown in 2008–2009 is likely to create the requirement for a plethora of new metrics within the financial services industry. The act initially applies to financial organizations, but it is reasonable to assume these provisions will find their way into other sectors that pose risks to the well-being of the economy as a whole. One of the provisions that are of interest to information security is the requirement to form a risk committee that must include a risk management expert. As a consequence, it will become increasingly difficult for management to ignore its responsibility for adequate protection of the organization’s assets, including information. In the coming years, we can expect to see interest in risk-related metrics becoming a greater priority and a reduction in the plausible deniability approach that has been common in times past—the “Goodness, I didn’t know we had those risks!” or “We don’t think cigarettes are addictive and cause lung cancer” executive defense. This statutory provision is summarized thus: “Financial services industry risk committees. This provision of the Dodd-Frank Act calls for certain nonbank, public financial companies and certain public bank holding companies to form a separate risk committee. Based on the legislation, risk committees will be held responsible for risk oversight in the organization. They must include the appropriate number of independent directors, as determined by the board of governors, based on factors that include the nature and size of the organization. They also are required to include at least one risk management expert, as defined by the act” (Deloitte 2010).

Fifty-eight percent of executives polled said [their organizations] have lost sensitive personal information, and for nearly 60 percent of those who have had a breach, it was not an isolated event.

Accenture (2009)
2.9 Summary

This chapter laid out a number of reasons explaining why information security metrics are so important for management, compliance, and so much more. Frankly, we struggle to understand how so many organizations claim to be front-runners in information security pursuant to the PWC Global State of Information Security 2012 study, yet decent security metrics are such a rare exception. It is difficult to understand what basis (any metrics, in fact) they have for believing themselves to be front-runners, other than wishful thinking.
## Contents

Foreword ........................................................................................................ xi
Preface .......................................................................................................... xiii
Acknowledgments ........................................................................................ xv
Office Memorandum ..................................................................................... xvii

1 Introduction ............................................................................................... 1
1.1 Why Have We Written This Book? .................................................... 2
1.2 What’s Different about This Metrics Book? ....................................... 3
1.3 Who Are We Writing This For? .......................................................... 5
1.4 Who Are We? ....................................................................................... 5
  1.4.1 W. Krag Brotby ......................................................................... 5
  1.4.2 Gary Hinson ............................................................................... 7
1.5 What We’ll Be Talking about ............................................................. 8
1.6 Defining Our Terminology ................................................................. 9
1.7 What We Expect of You, the Reader .................................................. 10
1.8 Summary............................................................................................... 11

2 Why Measure Information Security? ....................................................... 13
2.1 To Answer Awkward Management Questions .................................... 15
2.2 To Improve Information Security, Systematically ............................ 18
2.3 For Strategic, Tactical, and Operational Reasons ............................... 20
2.4 For Compliance and Assurance Purposes ......................................... 22
2.5 To Fill the Vacuum Caused by Our Inability to Measure Security ...... 23
2.6 To Support the Information Security Manager ................................. 24
2.7 For Profit! ............................................................................................ 25
2.8 For Various Other Reasons ............................................................... 26
2.9 Summary............................................................................................... 27

3 The Art and Science of Security Metrics ............................................... 29
3.1 Metrology, the Science of Measurement ........................................... 30
3.2 Governance and Management Metrics ............................................. 30
3.3 Information Security Metrics ..........................................................32
3.4 Financial Metrics (for Information Security) ..............................33
3.5 (Information Security) Risk Management Metrics .....................35
3.6 Software Quality (and Security) Metrics .................................36
3.7 Information Security Metrics Reference Sources .....................37
  3.7.1 Douglas Hubbard: How to Measure Anything (Hubbard 2010) ..................................................................37
  3.7.2 Andrew Jaquith: Security Metrics (Jaquith 2007) .................38
  3.7.4 Debra Herrmann: Complete Guide to Security and Privacy Metrics (Herrmann 2007) .....................40
  3.7.5 W. Krag Brotby: Information Security Management Metrics (Brotby 2009a) .......................................................41
  3.7.6 Lance Hayden: IT Security Metrics (Hayden 2010) ...............41
  3.7.7 Caroline Wong: Security Metrics: A Beginner’s Guide (Wong 2012) .............................................................42
  3.7.9 CIS Security Metrics (CIS 2010) ..............................................43
  3.7.10 ISACA .................................................................44
3.8 Specifying Metrics........................................................................46
3.9 Metrics Catalogs and a Serious Warning about SMD .................48
3.10 Other (Information Security) Metrics Resources .....................49
3.11 Summary .........................................................................................50

4 Audiences for Security Metrics ......................................................51
  4.1 Metrics Audiences Within the Organization .............................52
    4.1.1 Senior Management ............................................................53
    4.1.2 Middle and Junior Management ..........................................54
    4.1.3 Security Operations ............................................................55
    4.1.4 Others with Interest in Information Security ......................56
  4.2 Metrics Audiences From Without the Organization ..................57
  4.3 Summary .........................................................................................58

5 Finding Candidate Metrics ..............................................................59
  5.1 Preexisting/Current Information Security Metrics ...................60
  5.2 Other Corporate Metrics ............................................................61
  5.3 Metrics Used in Other Fields and Organizations .....................66
  5.4 Information Security Metrics Reference Sources .....................67
  5.5 Other Sources of Inspiration for Security Metrics ....................68
    5.5.1 Security Surveys ...............................................................68
    5.5.2 Vendor Reports and White Papers ......................................69
    5.5.3 Security Software ............................................................70
5.6 Roll-Your-Own Metrics ................................................................. 70
5.7 Metrics Supply and Demand ..................................................... 71
5.8 Summary .................................................................................... 72

6 Metametrics and the PRAGMATIC Approach ............................. 75
6.1 Metametrics .............................................................................. 76
6.2 Selecting Information Security Metrics ...................................... 78
6.3 PRAGMATIC Criteria ................................................................. 81
   6.3.1 P = Predictive ................................................................. 82
   6.3.2 R = Relevant .................................................................. 85
   6.3.3 A = Actionable .............................................................. 86
   6.3.4 G = Genuine ................................................................ 87
   6.3.5 M = Meaningful ............................................................ 88
   6.3.6 A = Accurate .................................................................. 90
   6.3.7 T = Timely ................................................................... 91
   6.3.8 I = Independent ............................................................. 93
   6.3.9 C = Cost ..................................................................... 94
6.4 Scoring Information Security Metrics against the PRAGMATIC Criteria ......................................................... 95
6.5 Other Uses for PRAGMATIC Metametrics .................................. 104
6.6 Classifying Information Security Metrics ................................... 105
   6.6.1 Strategic/Managerial/Operational (SMO) Metrics Classification ..................................................... 106
   6.6.2 Risk/Control Metrics Classification .................................... 108
   6.6.3 Input–Process–Output (Outcome) Metrics Classification ...................................................... 108
   6.6.4 Effectiveness and Efficiency Metrics Classification .......................................................... 109
   6.6.5 Maturity Metrics Classification .......................................... 109
   6.6.6 Directness Metrics Classification ........................................ 110
   6.6.7 Robustness Metrics Classification ........................................ 110
   6.6.8 Readiness Metrics Classification ......................................... 111
   6.6.9 Policy/Practice Metrics Classification ................................... 112
6.7 Summary .................................................................................... 113

7 150+ Example Security Metrics .................................................... 115
7.1 Information Security Risk Management Example Metrics ............. 118
7.2 Information Security Policy Example Metrics .............................. 130
7.3 Security Governance, Management, and Organization Example Metrics .............................................................. 140
   7.3.1 Information Security Financial Management Metrics ............ 141
   7.3.2 Information Security Control-Related Metrics ....................... 141
   7.3.3 Metrics for Business Alignment and Relevance of Controls .................................................. 142
   7.3.4 Control Monitoring and Testing Metrics ............................... 143
   7.3.5 Financial Information Security Metrics ................................. 156
7.4 Information Asset Management Example Metrics .............................................160
7.5 Human Resources Security Example Metrics ..............................................164
7.6 Physical Security Examples ...........................................................................179
7.7 IT Security Metric Examples ..........................................................................188
7.8 Access Control Example Metrics ..................................................................203
7.9 Software Security Example Metrics ..............................................................208
7.10 Incident Management Example Metrics ......................................................217
7.11 Business Continuity Management Examples .............................................225
7.12 Compliance and Assurance Metrics Examples ..........................................232
7.13 Summary ........................................................................................................244

8 Designing PRAGMATIC Security Measurement System .................................245
8.1 Brief History of Information Security Metrics ...............................................246
8.2 Taking Systems Approach to Metrics ............................................................248
8.3 Information Security Measurement System Lifecycle ....................................249
8.4 Summary ........................................................................................................266

9 Advanced Information Security Metrics ..........................................................267
9.1 High-Reliability Metrics ..................................................................................268
9.2 Indicators and Proxies ......................................................................................271
9.3 Key Indicators .................................................................................................272
9.3.1 Key Goal Indicators (KGIs) ......................................................................272
9.3.2 Key Performance Indicators (KPIs) ...........................................................273
9.3.3 Key Risk Indicators (KRIs) ......................................................................274
9.3.4 Critical Success Factors (CSFs) .................................................................275
9.4 Targets, Hurdles, Yardsticks, Goals, Objectives, Benchmarks, and Triggers .................................................................275
9.5 Summary ........................................................................................................277

10 Downsides of Metrics ........................................................................................279
10.1 Numbers Don’t Always Tell the Whole Story ..............................................279
10.2 Scoring Political Points through Metrics ......................................................281
10.3 Implausible Deniability ..................................................................................282
10.4 Metrics Gaps ..................................................................................................283
10.5 On Being Good Enough ................................................................................284
10.6 What Not to Measure .....................................................................................285
10.7 Summary ........................................................................................................287

11 Using PRAGMATIC Metrics in Practice .........................................................289
11.1 Gathering Raw Data .......................................................................................290
11.1.1 Sampling ..................................................................................................290
11.1.2 Automated Data Sources .......................................................................291
11.1.3 Observations, Surveys, and Interviews ...................................................293
11.1.4 Online or In-Person Surveys ..................................................................294
## Contents

Level 1–Initial ........................................................................................................... 385  
Level 2–Repeatable ................................................................................................ 386  
Level 3–Defined ..................................................................................................... 386  
Level 4–Managed .................................................................................................. 386  
Level 5–Optimizing ............................................................................................... 387  

Appendix D: Example Opinion Survey Form .......................................................... 389  
Security Awareness Survey on Malware .................................................................. 389  

Appendix E: SABSA Security Attributes Table ...................................................... 391  
Appendix F: Prototype Metrics Catalog ................................................................. 411  
Appendix G: Effect of Weighting the PRAGMATIC Criteria .................................. 427  
Appendix H: ISO27k Maturity Scale Metrics ......................................................... 431  
Appendix I: Sample Management Survey ............................................................... 475  
Appendix J: Observer Bias ..................................................................................... 477  
Appendix K: Observer Calibration ......................................................................... 481  
Appendix L: Bibliography ....................................................................................... 483  
Index ...................................................................................................................... 487
Information assurance (IA) has suffered for decades from the lack of sound quantitative methods for coping with risk and evaluating alternative strategies for allocating resources wisely in the fight against errors and attacks on our information systems.

All of us involved in IA maneuver through competing frameworks for choosing and implementing defenses; unfortunately, all too often we rely on the equivalent of word-of-mouth recommendations—industry best practices—in choosing particular paths. As our field matures, we must learn from other professions where methods for evaluating the quality of approaches have shifted from purely intuitive approaches to more systematic and repeatable methods.

The authors of this book have contributed their experience and creativity to present a valuable methodology for creating and evaluating elements of security management. Throughout the work, they emphasize how important it is to use heuristics rather than rigid rules in any field that changes constantly.

Security of all kinds suffers from the fundamental difficulty that if security measures work, there’s less evidence that the measures were necessary, at least for non-professional observers such as non-technical managers. Without sound metrics, we are in the position of passersby who encounter a man swinging plucked chickens around his head while he stands on a street corner: asked why he is doing that, he answers, “To keep the flying elephants away.” “But there are no flying elephants,” respond the befuddled observers. He crows triumphantly, “See? It works!”

Without defining, testing, and refining metrics, our profession will continue to be subject to the legitimate question, “How do you know?” How do we know if our proposals—our proposed spending, our proposed topology, our proposed changes—are reasonable? Why do we choose one set of responses over another? And how will we measure the results of our methods to evaluate their effectiveness and their efficiency?

In addition to supporting the development of IA, the methods presented in this text will reach professionals in fields that will benefit from good, PRAGMATIC metrics.
Thanks to W. Krag Brotby and Gary Hinson, I expect to see dramatic changes in our ability to analyze our security options, explain our choices, and measure our results.

M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business Management
Norwich University, Northfield, Vermont
Preface

Does your organization have a meaningful, worthwhile suite of information security measurements in place? No? Well then how exactly are you managing your information security risks and controls? Let’s guess: a pinch of good practices, a sprinkling of international standards, and a large measure of gut feel?!

Whereas most previous publications in this field have been either academic or narrow in scope, we have developed an eminently practical and rational approach to selecting information metrics that work. At its heart, the PRAGMATIC method is simply a tool to identify which of the thousands of possible security metrics are actually worth adopting. That claim may seem trivial if you have not personally struggled with this very issue, but trust us, it’s a Big Deal. Sifting the wheat from the chaff is never easy, but at least now we have a way to differentiate grains from husks. Hitherto, they all looked much the same—a uniformly bland shade of brown. PRAGMATIC security metrics appear in full glorious Technicolor™, and not merely 2D or 3D but 9D!

Writing this book was a surprisingly enjoyable labor. We came together serendipitously at a Wellington hotel in New Zealand where both of us just happened to be working on security metrics—Krag delivering a two-day metrics course, Gary co-leading a one-day metrics workshop for the local ISACA chapter. We instantly realized we had a lot in common, not least a sense of humor and a love of fine red wine that made our first encounter a memorable experience. Our shared passion for information security metrics and the belief that there has to be a better way drove us together in the search for enlightenment.

Our decision to co-author this book was momentous, not least for the fact that although Krag had already written books on information security governance and metrics, the only book Gary had written was his PhD thesis—many moons ago, and on microbial genetics at that!

At the time we agreed to collaborate, we had not invented PRAGMATIC. The PRAGMATIC concept mysteriously emerged from our early discussions, initially as a way to align our thoughts, but it soon became evident that we had chanced upon something uniquely valuable. The process of evaluating, comparing between, considering, and eventually choosing security metrics solved a vexatious problem.
affecting practically everyone who gets into security metrics. Simply stated, we stumbled on the way to answer the deceptively simple/naïve question, “What should we measure?” and that answer, in turn, opened up entirely new horizons. Many previously intractable information security management problems become solvable through PRAGMATIC metrics, or rather through the availability of meaningful, factual data on which to base important decisions.

Aside from information security, we are intrigued at the prospect of using the PRAGMATIC approach to develop and select worthwhile metrics in different fields of management—not just closely allied areas such as governance, risk management, and compliance but almost anything in fact. If you are an expert in sports management, financial management, HR management, engineering management, strategic management, or some other specialty who is inspired by this book to develop PRAGMATIC metrics in your context, please do get in touch with the authors through www.SecurityMetametrics.com. We’d love to work with you on this.