INFORMATION SECURITY GOVERNANCE
A Practical Development and Implementation Approach

Krag Brotby
INFORMATION SECURITY
GOVERNANCE
INFORMATION SECURITY GOVERNANCE
A Practical Development and Implementation Approach

Krag Brotby

WILEY
A JOHN WILEY & SONS, INC., PUBLICATION
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgments</td>
<td>xi</td>
</tr>
<tr>
<td>Introduction</td>
<td>xiii</td>
</tr>
<tr>
<td><strong>1. Governance Overview—How Do We Do It? What Do We Get Out of It?</strong></td>
<td>1</td>
</tr>
<tr>
<td>1.1 What Is It?</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Back to Basics</td>
<td>2</td>
</tr>
<tr>
<td>1.3 Origins of Governance</td>
<td>3</td>
</tr>
<tr>
<td>1.4 Governance Definition</td>
<td>5</td>
</tr>
<tr>
<td>1.5 Information Security Governance</td>
<td>5</td>
</tr>
<tr>
<td>1.6 Six Outcomes of Effective Security Governance</td>
<td>6</td>
</tr>
<tr>
<td>1.7 Defining Information, Data, Knowledge</td>
<td>7</td>
</tr>
<tr>
<td>1.8 Value of Information</td>
<td>7</td>
</tr>
<tr>
<td><strong>2. Why Governance?</strong></td>
<td>9</td>
</tr>
<tr>
<td>2.1 Benefits of Good Governance</td>
<td>11</td>
</tr>
<tr>
<td>2.1.1 Aligning Security with Business Objectives</td>
<td>11</td>
</tr>
<tr>
<td>2.1.2 Providing the Structure and Framework to Optimize Allocations of Limited Resources</td>
<td>12</td>
</tr>
<tr>
<td>2.1.3 Providing Assurance that Critical Decisions are Not Based on Faulty Information</td>
<td>13</td>
</tr>
<tr>
<td>2.1.4 Ensuring Accountability for Safeguarding Critical Assets</td>
<td>13</td>
</tr>
<tr>
<td>2.1.5 Increasing Trust of Customers and Stakeholders</td>
<td>14</td>
</tr>
<tr>
<td>2.1.6 Increasing the Company’s Worth</td>
<td>14</td>
</tr>
<tr>
<td>2.1.7 Reducing Liability for Information Inaccuracy or Lack of Due Care in Protection</td>
<td>14</td>
</tr>
<tr>
<td>2.1.8 Increasing Predictability and Reducing Uncertainty of Business Operations</td>
<td>15</td>
</tr>
<tr>
<td>2.2 A Management Problem</td>
<td>15</td>
</tr>
</tbody>
</table>
11. Sample Strategy Development

11.1 The Process

12. Implementing Strategy

12.1 Action Plan Intermediate Goals
12.2 Action Plan Metrics
12.3 Reengineering
12.4 Inadequate Performance
12.5 Elements of Strategy
   12.5.1 Policy Development
   12.5.2 Standards
12.6 Summary

13. Security Program Development Metrics

13.1 Information Security Program Development Metrics
13.2 Program Development Operational Metrics


14.1 Management Metrics
14.2 Security Management Decision Support Metrics
14.3 CISO Decisions
   14.3.1 Strategic Alignment—Aligning Security Activities in Support of Organizational Objectives
   14.3.2 Risk Management—Executing Appropriate Measures to Manage Risks and Potential Impacts to an Acceptable Level
   14.3.3 Metrics for Risk Management
   14.3.4 Assurance Process Integration
   14.3.5 Value Delivery—Optimizing Investments in Support of the Organization’s Objectives
   14.3.6 Resource Management—Using Organizational Resources Efficiently and Effectively
   14.3.7 Performance Measurement—Monitoring and Reporting on Security Processes to Ensure that Organizational Objectives are Achieved
14.4 Information Security Operational Metrics
   14.4.1 IT and Information Security Management
   14.4.2 Compliance Metrics

15. Incident Management and Response Metrics

15.1 Incident Management Decision Support Metrics
   15.1.1 Is It Actually an Incident?
15.1.2 What Kind of Incident Is It? 157
15.1.3 Is It a Security Incident? 157
15.1.4 What Is the Security Level? 157
15.1.5 Are there Multiple Events and/or Impacts 158
15.1.6 Will an Incident Need Triage? 158
15.1.7 What Is the Most Effective Response? 158
15.1.8 What Immediate Actions Must be Taken? 158
15.1.9 Which Incident Response Teams and Other Personnel Must be Mobilized? 159
15.1.10 Who Must be Notified? 159
15.1.11 Who Is in Charge? 159
15.1.12 Is It Becoming a Disaster? 159

16. Conclusion 161

APPENDIX A. SABSA Business Attributes and Metrics 163

APPENDIX B. Cultural Worldviews 181
Heirarchists 181
Egalitarians 181
Individualists 182
Fatalists 182

Index 185
Acknowledgments

A debt of gratitude is acknowledged to my wife, Melody, who graciously accepted many late night hours in assembling this work. Also acknowledged are those who have supported this effort by giving their time to advise, review, and comment on this exposition, including ISACA associates of notable competence Bruce Wilkins, Gary Barnes, and Ron Hale; other professionals including Charles Neal, formerly of the FBI, and Adam Hunt, currently with Inland Revenue in New Zealand. Thanks are also due to John Sherwood and David Lynas from the United Kingdom for their assistance and support with the SABSA architectural material in this work. And finally, appreciation is due to my unusually helpful and cooperative publisher and staff in bringing this hopefully illuminating work to light.

K. B.
Introduction

For most organizations, reliance on information and the systems that process, transport, and store it, has become absolute. In many organizations, information is the business. Actionable information is the basis of knowledge and as Peter Drucker stated over a decade ago, “Knowledge is fast becoming the sole factor of productivity, sideling both capital and labor.”*

This notion is buttressed by recent studies showing that over 90% of organizations that lose their information assets do not survive. Research also shows that currently, information assets and other intangibles comprise more than 80% of the value of the typical organization.

Yet, even as this realization has belatedly started to reach executive management and the boardroom in recent years, organizations are plagued by evermore spectacular security failures and losses continue to mount. This is despite a dramatic a rise in overall spending on a variety of security- or assurance-related functions and national governments imposing a host of increasingly restrictive regulations.

This host of new security-related regulations has in turn led to a proliferation of the number and types of “assurance” functions. Until recently, for example, “privacy” officers were unheard of, as were “compliance” officers. Now, they and others, such as the Chief Information Security Officer, are commonplace. It should be noted that all assurance functions are an aspect of what is arbitrarily labeled “security” and, indeed, what is called “security” is invariably an assurance function. In turn, both are elements of risk management.

Not only has the diversity of “assurance” functions increased, the requirements for these activities in many of an organization’s other operations are now the norm. Examples include the HIPAA “privacy assurance” functions generally handled by Human Resources, or SOX disclosure compliance as a purview of Finance.

For many larger organizations, a list of assurance-related functions might include:

- Risk management
- BCP/DR
- Project office
- Legal

Combined, these assurance functions constitute a considerable percentage of an organizations’ operating budget. Yet, ironically, this increase in assurance functions has in many organizations led to a decrease in “safety” or security. This is a consequence of increasingly fragmenting assurance functions into numerous vertical “stovepipes” only coincidentally related to each other and to the organization’s primary business objectives. This, despite the fact that all of these activities serve fundamentally only one common purpose: the preservation of the organization and its ability to continue to operate and generate revenue.

To compound the problem, these functions invariably have different reporting structures, often exist in relative isolation, speak different languages, and more often than not operate at cross purposes. Typically, they have evolved over a period of time, usually in response to either a crisis du jour or to mounting external regulatory pressures. Their evolution has often involved arbitrary factors unrelated to improving security functionality, efficiency, or effectiveness.

As these specialized assurance functions have developed, national or global associations have formed to promote the specialty. One outcome of this “specialty”-centric perspective has been to widen the divide between elements of what should arguably be a continuous “assurance” process, seamlessly dovetailed and aligned with the business.

So what is the way forward? It has become increasingly clear that the solution lies in elevating the governance of the typical myriad assurance functions to the highest levels of the organization. Then, as with other critical, expensive organizational activities, an assurance governance framework must be developed that will integrate these functions under a common strategy tightly aligned with and supporting business objectives.

Alternatively, for most organizations, failure to implement effective information security governance will result in the continued chaotic, increasingly expensive, and marginally effective firefighting mode of operation typical of most security departments today. Tactical point solutions will continue to be deployed, and effective administration of security and integration of assurance functions will have no impe-
tus and remain merely a concept in the typically fragmented multitude of “assurance-” and security-related stovepipes. Allocation of security resources is likely to remain haphazard and unrelated to risks and impacts as well as to cost-effectiveness. Breaches and losses will continue to grow and regulatory compliance will be more costly to address. It is clear that senior management will increasingly be seen as responsible and legally liable for failing the requirements of due care and diligence. Customers will demand greater care and, failing to get it, will vote with their feet, and the correlation between security, customer satisfaction, and business success will become increasingly obvious and reflected in share value.

Against this backdrop, this book provides a practical basis and the tools for developing a business case for information security (or assurance) governance, developing and implementing a strategy to increasingly integrate assurance functions over time, improving security, lowering costs, reducing losses, and helping to ensure the preservation of the organization and its ability to operate.

Chapters 1 through 6 provide the background, rationale, and basis for developing governance. Chapters 7 through 14 provide the tools and an approach to developing a governance implementation strategy.

Developing a strategy for governance implementation will, at a high level, consist of the following steps:

1. Define and enumerate the desired outcomes for the information security program
2. Determine the objectives necessary to achieve those outcomes
3. Describe the attributes and characteristics of the desired state of security
4. Describe the attributes and characteristics of the current state of security
5. Perform a comprehensive gap analysis of the requirements to move from the current state to the desired state of security
6. Determine available resources and constraints
7. Develop a strategy and roadmap to address the gaps, using available resources within existing constraints
8. Develop control objectives and controls in support of strategy
9. Create metrics and monitoring processes to:
   - Measure progress and guide implementation
   - Provide management and operational information for decision support
Chapter 1

Governance Overview—How Do We Do It? What Do We Get Out of It?

1.1 WHAT IS IT?

Governance is simply the act of governing. The *Oxford English Dictionary* defines it as “The act or manner of governing, of exercising control or authority over the actions of subjects; a system of regulations.”

The relevance of governance to security is not altogether obvious and most managers are still in the dark about the subject. Information security is often seen as fundamentally a technical exercise, purely the purview of information technology (IT). In these cases, the information security manager generally reports directly or indirectly to the CIO but in some cases may report to the CFO or, unfortunately, even to Operations.

In recent years, there has also been an increase in the number of senior risk managers, or CROs, and, in some cases, Information Security reports through that office. Although these organizational structures often work reasonably well in practice, provided the purview of security is primarily technical and the manager is educated in the subject and has considerable influence, in many cases they do not work well and, in any event, these reporting arrangements are fundamentally and structurally deficient. This contention is often subject to considerable controversy even among security professionals. However, analysis of the wide range of activities that must be managed for security to be effective and study of the best security management shows that it requires the scope and authority equivalent to that of any other senior manager. To be effective, security and other assurance activities are regulatory functions and cannot report to the regulated without creating an unten-
able structural conflict of interest. Maintaining a distinction between regulatory and operational functions is critical, as each has a very different focus and responsibility. The former is related to safety and the latter to performance, and it is not unusual for tension to exist between them.

Part of the reason that the requirement for separation of security from operational activities is not evident is that the definitions and objectives of security generally lack clarity. Asking the typical security manager what the meaning of security is will elicit the shop-worn response of “ensuring the confidentiality, integrity, and availability of information assets.” Pointing out that that is what it is supposed to do, that is its mission, and not what it is, generally elicits a blank stare. Probing further into the objectives of security will usually result in the same answer.

The lack of clarity about what security should specifically provide, how much of it is enough, and knowing when that has been achieved poses a problem and contributes to the confusion over the appropriate organizational structure for security. Lacking clear objectives, a definition of success, and metrics about when it has been achieved begs the question, *What does a security manager actually do?* How is the manager to know when he or she is managing appropriately? What is his or her performance based on? How does anyone know?

In other words, as in any other business endeavor, we manage for defined objectives, for outcomes. Objectives define intent and direction. Performance is based on achieving the objectives. Metrics determine whether or not objectives are being achieved.

### 1.2 BACK TO BASICS

If there is a lack of clarity looking ahead, reverting to basics may help shed light on the subject. Security fundamentally means safety, or the absence of danger. So in fact, IT or information security is an assurance function, that is, it provides a level of assurance of the safety of IT or information. Of course, it must be recognized that the safety of an organization’s information assets typically goes a considerable distance beyond the purview of IT.

IT is by definition technology centric. IT security is by definition the security related to the technology. From a business or management perspective, or, indeed, from a high-level architectural viewpoint, IT is simply a set of mechanisms to process, transport, and store data. Whether this is done by automated machinery or by human processes is not relevant to the value or usefulness of the resultant activities. It should be obvious, therefore, that IT security cannot address the broader issue of information “safety.”

Information security (IS) goes further in that it is information centric and is concerned with the “payload,” not the method by which it is handled. Studies have clearly shown that the risks of compromise are often greater from the theft of paper than from IT systems being hacked. The loss of sensitive and protected information is five times greater from the theft or loss of laptops and backup tapes than it is from being hacked. These are issues typically outside the scope of IT security. The fact
that the information on these purloined laptops or tapes is infrequently encrypted is not a technology problem either; it is a governance and, therefore, a management problem.

To address the issues of “safety,” the scope of information security governance must be considerably broader than either IT security or IS. It must endeavor to initiate a process to integrate the host of functions that in the typical organization are related to the “safety” of the organization. A number of these were mentioned in the Introduction, including:

- Risk management
- BCP/DR
- Project office
- Legal
- Compliance
- CIO
- CISO
- IT security
- CSO
- CTO
- CRO
- Insurance
- Training/awareness
- Quality control/assurance
- Audit

To this list we can add privacy and, perhaps more importantly, facilities. Why facilities? Consider the risks to information “safety” that can occur as a function of how the facility operates: the physical security issues, access controls, fire protection, earthquake safety, air-conditioning, power, telephone, and so on. Yet, risk assessments in most organizations frequently do not consider these elements.

The advantage of using the term “organizational safety” and considering the elements required to “preserve” the organization is that the task of security management becomes clearer. It also becomes obvious that many of the other “assurance” functions that deal with aspects of “safety” must be somehow integrated into the governance framework. It also becomes clear that most attempts to determine risk are woefully inadequate in that they fail to consider the broad array of threats and vulnerabilities that lie beyond IT and, indeed, beyond IS as well.

1.3 ORIGINS OF GOVERNANCE

It may be helpful to consider how the whole issue of governance arose to begin with to understand its relevance to information security. The first instance of the appear-