



# Business Aligned Security

October 2009



© 2009 Edgile, Inc – All Rights Reserved

## Introduction

Information security is viewed by most organizations as a risk mitigation activity. This view has been reinforced by the security professionals, governance processes, and security approaches used. The information security profession grew out of the audit profession, compliance and regulatory groups, and public security agencies, which has reinforced the risk-centric view of security. However, today information security plays a very important role in enabling the business. Security groups have not been highly effective at driving the necessary funding and security activities needed to adequately protect information resources. Most organizations are littered by security point solutions deployed as reactions to events as opposed to a proactive, effective security strategy.

This paper discusses a new approach to security governance that moves an organization's information security group from a risk-centric function to a business aligned capability, helping to transform how security is viewed and funded within the enterprise. The risk-centric and business aligned approaches are not mutually exclusive and both are important, but today security groups are primarily risk-centric in their approaches. An enhanced focus on a business aligned approach will elevate security from a purely risk mitigation activity to a strategic business enabler for the enterprise.

## The Information Landscape

The future information landscape is dotted with cloud computing infrastructure, virtual global workforces, information at your fingertips, and dynamic collaboration technologies. The need to compete and win in the market, reduce cost, and spur innovation is driving organizations down this envisioned road. This change has been taking place slowly over the past 10 years but the pace has increased

as major software vendors, technology organizations and service providers jump into the market with solution offerings. With this changing landscape, security looms as either a major business enabler or an insurmountable roadblock. Security organizations will not stop this trend, and if they are viewed as a roadblock, they will be ignored except in the most risk-centric organizations. In this new world, a viable option exists for security organizations, one of *Strategic Enabler*. Security can be positioned to enable movement towards the new



information landscape. Security organizations need to align with the business and senior management, drive the necessary funding to support these efforts, and implement effective solutions to manage risk as organizations make this transformation.

## Risk-Based Security vs. Business Aligned Security

Today, organizations typically use a risk-centric approach to drive security activities and investments. In theory, the risk approach starts with vulnerabilities, threats and related risks and then mitigating controls are evaluated and implemented to reduce risk exposure. The security organization's goal under this approach is to manage an organization's risk exposure to an acceptable level.

A *Business Aligned Security* approach starts with the business, its strategy and its goals to ultimately build a security strategy that supports and enables the business while minimizing the additional exposure these business activities will create. The differences between these two approaches to security are significant.

### Risk-Based Approach

The risk-based approach, which has driven information security for years, starts with understanding the risks facing the organization. In recent years, organizations have started to use one of several standard frameworks to identify mitigating controls then working to align these controls to risks instead of truly going through a risk-based evaluation approach. *Control Objectives for Information and related Technology (COBIT®)*

and ISO 27001 / 27002 are examples of two standard frameworks. Each risk factor is first valued in some manner and then existing mitigating controls are used to adjust the risk factor which provides the exposure for that area ( $\text{Risk} - \text{Mitigating Controls} = \text{Exposure}$ ). Once all the exposures are identified, one can plan how to add mitigating controls to further manage the organization's exposure.

This approach creates two major issues. First, many business managers perceive mitigating controls as roadblocks. Second, security organizations struggle to value the exposure in a meaningful way to business managers. As a result, a trend is emerging that establishes an organization's security direction based on standard control frameworks, Best Practice, and compliance requirements. The approach does produce results, but generally favors point solutions as opposed to broad strategies. This can be successful at layering security across



the organization, but it has not been effective at driving significant funding, aligning security with the business or gaining support from senior executives. The risk-centric approach needs to be supplemented with a stronger business focus, which can be achieved with a *Business Aligned Security* approach.

## Business Aligned Security Approach

The *Business Aligned Security* approach starts with the business strategy and business goals. These are usually well defined and communicated from the firm's senior leadership and are interpreted and executed by the organization in a wide range of manners. An example would be a firm seeking to grow global market share by 10 percent while cutting costs by 10 percent. The organization's execution strategy could include increasing the number of foreign sales offices, enhancing collaboration capabilities with a 3<sup>rd</sup> party sales force, or moving to Software as a Service (SaaS) to lower IT costs. The security organization



first needs to clearly understand the approach and the tactics of how the organization plans to execute the strategy. Many of the tactics will be similar in nature. For example, you might have a number of groups looking to move to a SaaS model to support needed capabilities. The goal is to categorize the tactical execution around significant strategic capabilities.

To successfully execute the business strategy, information security plays a key role in ensuring that strategic capabilities are securely planned, developed, and implemented. Strategic capabilities can include an enhanced collaboration capability, a virtual global office capability, or a cloud computing capability. Many, if not most, of the strategic capabilities will depend heavily on a security foundation. Accordingly, an enhanced, secure collaboration capability is needed instead of solely an enhanced collaboration capability. These strategic capabilities become the drivers for a *Business Aligned Security* strategy. Components of the *Business Aligned Security* strategy can include an enhanced identity management environment to support SaaS service providers. Another example is the use of digital rights technology to support secure collaboration with 3<sup>rd</sup> parties. Each component of the *Business Aligned Security* strategy must be clearly tied back to the required strategic capabilities and ultimately to the business strategy.

The development of the *Business Aligned Security* strategy is driven by the business strategy and strategic business capabilities. The process of developing the strategy requires a significant amount of interaction with the business. Defining the strategic capabilities, clearly from a security perspective, is done in conjunction with the business and IT groups. This interaction is critical to the process and facilitates the alignment between the security groups and business.

The process of developing a *Business Aligned Security* strategy is a 2-3 month process for most organizations. The process requires business savvy security professionals primarily focused on making the business successful, in addition to managing risk.

## Benefits

Typically, the *Business Aligned Security* strategy produces improved results compared to a risk-centric only approach. Enhancing the current set of mitigating control that a risk-centric approach focuses on is still an important function but is an operational activity. The *Business Aligned Security* approach is a strategic activity focused on enabling the business strategy and strategic capabilities in a secure manner. By placing a larger focus on the business, the organization's exposure will be lowered while providing greater benefits to the business. For example, broader security questions are asked, such as "how can we securely enable cloud computing?" The results produce strategic solutions not considered when using the risk-centric

approach. The strategic solutions solve broader problems and address future risk. However, the most valuable benefit is that business starts to clearly view security as a strategic enabler. The conversation between the business and security organization moves from a risk discussion to a strategic discussion and security is addressed earlier in the strategy and planning processes. This new level of partnership and alignment also simplifies the budget request process and gains support for increased spending on security activities. Moving to a *Business Aligned Security* approach can greatly benefit the business and its security organization.

### Benefits of a Business Aligned Security Strategy

- Security strategy clearly aligned with the business strategy
- Close alignment between funded corporate initiatives and security initiatives
- Forward-looking security strategy
- Fewer point solutions / more strategic security initiatives
- Better justification for funding security initiatives
- The view of security is elevated to being a strategic enabler

## Conclusion

A *Business Aligned Security* strategy and a risk-based strategy are not mutually exclusive. Organizations will need to continue to manage their overall risk profile, but this is an ongoing activity that is not designed to address the opportunities confronting business today. Security organizations must do a better job of communicating the value of security to the business and its impact on the bottom line. The *Business Aligned Security* approach is an effective methodology to develop alignment between the security organization and the business, communicate the value of security to executives and help justify expanding security funding.

## About Edgile

Edgile was established in 2001 by a team of partners and senior managers from Deloitte to deliver Strategic Security Services to Fortune 500 organizations. Edgile's unique *Business Aligned Security* approach has helped drive major security efforts from conception, to funding, to deployment successfully. Our long-term relationship with leading organizations speaks to our success.



## About the Authors



**Don Elledge: CEO** | [don.elledge@edgile.com](mailto:don.elledge@edgile.com)

Don is Edgile's Chief Executive Officer and brings a broad background in business and technology. He has advised leading companies in the areas of Technology, Strategy, Governance and Security. He has built and led large successful organizations. Before Edgile, Don's was a partner at Deloitte and worked at First Boston in investment banking. Don is formally educated in business, economics and finance. His loyalty to people is reflected in the talented and experienced teams he has built at Deloitte and Edgile, as well as the long-term relationships he has developed with Fortune 500 companies.



**Roin Nance: COO** | [roin.nance@edgile.com](mailto:roin.nance@edgile.com)

Roin brings over 22 years of experience in IT Infrastructure Planning and Deployment, Financial Planning and Management, Business Systems Design, Implementation and Management, Strategic Planning, Quality Assurance Program Design and Implementation, Performance and Operational Auditing. Roin was a senior manager at Deloitte before joining Edgile. He is a Lieutenant Colonel in the U.S. Air Force Reserve and holds a Top Secret, SCI Clearance. Roin is a Certified Information Systems Auditor (CISA) and a Certified Public Accountant (CPA).