“Developing a Security Strategy”
—an excerpt from Security Battleground

www.securitybattleground.com

Available on amazon.com
Developing a Security Strategy

Abstract

When called to participate in a strategic planning process, often the typical planning session is more focused on security gap analysis than on developing a true strategic plan for security. Put simply, the typical security team, for various valid reasons, audits the environment for its ability to defend against generic threats or attacks, and, where they see holes in their existing controls, they develop a plan to plug them. The resulting roll-out plan isn’t a strategic plan because it’s missing a key ingredient: an explicit understanding of the company’s assets that need to be protected. Without this ingredient, security planners cannot judge whether controls are adequate, inadequate, or unnecessarily sophisticated. Without an alignment between specific business risks and security controls, the roll-out plan cannot be optimized. This article examines what is involved in developing a world-class security strategy.

The call to participate in the strategic planning process is one of the most challenging requests for a security analyst. Interestingly, the typical planning session is more focused on gap analysis than on developing a true strategic plan. Put simply, the typical security team, for various valid reasons, audits the environment for its ability to defend against generic threats or attacks, and, where they see holes in their existing controls, they develop a plan to plug them.

The resulting roll-out plan isn’t a strategic plan because it’s missing a key ingredient: an explicit understanding of the company’s assets that need to be protected. Without this ingredient, security planners cannot judge whether controls are adequate, inadequate, or unnecessarily sophisticated. Without an alignment between specific business risks and security controls, the roll-out plan cannot be optimized.

The security team has to build a bridge with the lines of business (LOBs). LOBs describe how companies are organized. For some companies, LOBs are profit centers offering different types of products and services. In the financial services industry, for example, the online banking group and the consumer finance groups are two typical lines of business. LOBs can also be functional groups such as human resources or finance. The success of a security organization depends heavily upon its relationships with LOBs or, more specifically, LOB leaders.

In an atypical planning session, the Chief Security Officer (CSO) didn’t kick off the session with an inventory of security controls and potential threats; instead, he spent the first day discussing how the business is changing and how the security posture would need to be adjusted because of changes in the impact of different business risks. Note that he did not focus on business risks in isolation, but rather on the harm that different types of breaches would cause for the company.

It turns out that the CSO had been working with LOB leaders so that he could recognize and capture business risks and their impacts from those who know them best. He used business terms, not security terms. “What could go wrong and cause trouble for your LOB?” he asked. “What would the impact be on your business?” It was this information that allowed the CSO to spend the first day describing the business in detail. On the second day, we reviewed the current security posture in the context of business risks and their impacts. More specifically, the CSO
asked his security team to estimate the likelihood of a breach, given their current set of controls for areas that had large negative business risks.

For example, one LOB leader revealed that he was planning to launch a new customer outreach campaign that would result in a large customer database. In addition, his plans called for the ability of the sales people to access this database via mobile devices. Loss of that information contained in the database would wreak havoc for both the LOB and the company as a whole. This would be a change in business practices that the security organization should be aware of.

The CSO’s methodology guaranteed that the security strategy was aligned with business. While some business practices require improved protection, other practices are less demanding. The security team was able to optimize the application of its resources. The methodology also allowed the CSO to explain the strategic investments that his group was recommending by specifically tying them to LOB risk and impact.

This company understands that blanket protection by way of a technology-centric gap analysis results in security systems that are misaligned with the company’s business risk profile. For this company, business risk and the security plan fit together like a dovetail joint.

**Real Strategic Planning**

The essence of real strategic planning is quite simple; just figure out where you are and where you want to be, and then figure out when and how to get there. But while the essence is simple, building a proper strategic plan for security takes thoughtful effort.

World-class businesses build and maintain strategic plans for much of what they do. Strategic planning drives everything from capital investments, product development, services offerings, and marketing efforts to sales initiatives. Strategic plans define the need for action, the impact of that action, and the driving forces behind the actions. In other words, the plans define what will be done without stating how it will be done. Strategic plans also identify key indicators that can be measured and managed along the way to ensure that the plan is on track. These are serious plans with real consequences for the enterprise.

Strategic plans also set expectations for executives. Executives are most interested in the investment needed to execute the plan and the expected returns. In many ways, the strategic plan
and its accompanying budget form a contract between executive management and the organization as a whole. In another sense, the strategic plan is a battle plan, and everyone has marching orders.

In our experience, security organizations rarely have complete and updated strategic plans. For some organizations, tactical reactions to incidents are the norm. The so-called plan is to react after a breach, which is, of course, no plan at all. A security organization manager recently told us, “This is my plan but, as always, I am a breach away from changing it.” The security manager was not kidding. This was how his organization operated. He was forced to use the last breach to get the funding and backing needed to make a change in the organization. He did not want to work this way, but he had found over the years that this approach generated the support he needed to make an improvement, even if it was a bit random at times.

**Strategic Planning for Security**

The typical security organization is buried inside the IT group, which is viewed as a service function in most businesses. Often, LOB leaders view IT—including security—as an inhibitor to speed and agility. The security team’s obligation to draw out the harsh realities of doing business in the middle of a cyber battleground often puts it at odds, either in theory or by perception, with the LOBs that it supports, making it more difficult to build a real strategic plan. Imagine a military strategist trying to draw up a battle plan in the absence of key information, such as whom they would be fighting, and what troops and support they could count on.

Isolation from business operations leaves strategic planners with a void at the most crucial step in the planning process: direction. Without an understanding of LOB operations, planners are forced to derive the direction for the security plan from a gap analysis, which is simply preparing an inventory of current countermeasures and filling gaps where protection is lacking. Each gap in the armor is placed on a list and then, as budget allows, the holes are plugged.

On the surface, the gap analysis approach looks good and seems quite reasonable. However, when we analyze gaps in security at typical companies, the investment in armor seldom aligns with the amount of protection needed. When performed in isolation without direction from LOB leaders, gap analysis encourages a breach-by-breach approach that cannot, by definition, be considered strategic.

**Business Risk is the Foundation**

Strategic planning for security must begin with an analysis of the business. The security organization remains responsible for mastering the technologies that protect the company’s assets, but what the security organization cannot do by itself, however, is build and maintain an understanding of the enterprise lines of business, their most important information assets, and the multitude of security-oriented business risks that need to be identified and mitigated.

Without this understanding of the bigger picture, security often falls prey to what we call the shiny new tool syndrome; when a new threat emerges, the organization responds by acquiring the latest new security product on the market. This technology-centric approach is typically the hallmark of an organization that hasn’t based its strategic plan on an understanding of business risks.

Imagine being asked to design a security system for Fort Knox without knowing exactly what the system should be protecting or lacking a clear understanding the value of those assets. Would
you be able to build the appropriate protections? Security strategists need to know the value of the assets they are protecting and the real cost of breaches in order to determine current and future security requirements. For example, protecting customer identity data should be a higher priority than protecting other types of data that may have less serious negative consequences.

**A Common Language**

The solution to this challenge is to entice LOB leaders into playing a key role in the strategic planning process. We say “entice” because over the years engaging business leaders has not always been easy. The relationship between security and the LOB has been strained because security has been seen as a function that limits agility and bogs down the various business processes. However, with recent high-profile breaches that have had disastrous financial consequences LOB leaders are much more motivated to participate in strategic planning for enterprise security.

A starting point in establishing a cooperative relationship with business leaders is to demonstrate that the security organization understands the concerns and viewpoint of LOB leaders. The language of business should be the common language for the security team and the LOB leaders.

As we said, most security organizations do not have security plans aimed at mitigating business risks specific to the enterprise. Generally, what they consider strategic planning is either uninformed or under-informed by LOB leaders.

From an IT perspective, for example, databases vary in requirements for capacity, performance, and availability, but when comparing Service Level Agreements (SLAs) of one database versus another, the risks associated with the value of the content may be overlooked.

However, from a business-risk perspective, a database holding customer payment information is vastly more valuable than a database containing external documents otherwise available in the public domain.

Without aligning security strategy with business risk, the security organization is implicitly expected to deliver complete protection on a fixed budget, an assumption that puts the security organization in an unenviable position. Risks can be mitigated, and vulnerabilities can be remedied, but it’s not as simple as accepting the request, “Just make the enterprise secure.”

In fairness to business leaders, however, we understand that it is difficult to determine the correct level of funding. If a well-secured business is not financially viable, there will soon be nothing to protect.

**A Model for Planning Security Strategy**

The most common missing piece in strategic security planning for many organizations is an understanding of the key elements of the business. Understanding generic threats and vulnerabilities is important, but understanding which of these threats and vulnerabilities impact a particular organization more severely is vital.

Our model for strategic security planning is shown in Figure 1. To help the security team bridge the gap between the lines of business and security controls, we prescribe a model based on an understanding of business risks. All security-related decisions trace back to business value and business risk. This article focuses on the overall process. A complete discussion of each of the stages can be found in the book *Security Battleground: An Executive Field Manual*. 
The first phase in planning security strategy is aimed at gaining an understanding of the business, its assets, risks, and regulations. When information gathering is complete, the security team then performs an analysis to identify and prioritize enterprise riches that must be well protected, risks that must be mitigated to avoid ruin, and the compliance requirements that apply to the enterprise.

In the second phase of the planning process, a prioritized list of business risks associated with assets, potential threats, and regulations is transformed into an inventory of threat vectors and compliance deficiencies.

In the third and final phase, we identify deficient areas of our protection that are associated with significant risk. We prioritize these findings and determine what can be digested by the organization. During this process, we make a concerted effort to understand the benefits that can be obtained from an optimization initiative, not just security posture improvements.

When assembled correctly, each control identified in the strategic plan is linked directly to business risks. In this way, we can balance the degree of risks with the investment in controls. Our goal is to avoid planning for controls that merely improve overall security in favor of a model that matches controls to the risk profile of the business.

**Recognizing and Capturing Risk**

LOB leaders are the primary sources for understanding the business. These individuals know that their business depends on IT systems, and they know that not all systems are equally valuable.
LOB leaders understand what information they depend on, what can be done with sets of information, and how different sets of information interact with each other.

These LOB leaders are critical members of the security organization’s strategy team—although they might not know it. They are not security experts, so conversations with LOB leaders should focus on LOB risks and not security technologies. To these individuals, we pose three key questions, using their own language:

- **What could make a hacker rich?**
  What information in your business could be stolen and sold for considerable gain? Customer identity data is an example of information that can be sold on the black market. There is a market for intellectual property such as manufacturing secrets, key chemical compounds, bidding information, and merger-and-acquisition plans.

- **How can your company be ruined?**
  What events could cause material or even irreparable harm to your business? For example, a denial-of-services attack on an ecommerce site can halt a company’s ability to transact business with its customers. Exposing a company’s customer base can tarnish the brand of the company and its ability to retain and gain customers.

- **What are the company’s regulatory obligations?**
  Due to changes in the business environment, what new rules and procedures must the company follow? For example, a company expanding to offer management services for patient healthcare information will need to comply with the Health Insurance Portability and Accountability Act (HIPAA) regulations. Often the expansions of an existing company into new geographical regions will cause significant regulatory impact.

These questions can lead LOB leaders to reveal critical information about which business assets are valuable and need to be well protected. LOB leaders can then estimate the impact on their businesses if a loss were to occur.

Once again, the questions are purposefully non-technical to lead LOB leaders away from discussions of security technologies and policies and in the direction of discussing business assets, risks, and the impact of losses. When you speak a common language, LOB leaders actually enjoy explaining how their businesses work.

**Examples of Business Risk**

While each enterprise will have its own constellation of business risks, here are some common themes based on our experience in the field.

*Reputational risk*: Trust in an enterprise is compromised. When hackers breach an email system, for example, and publish correspondence among members of the board of directors, the harm is the embarrassment to the organization and the increased concern customers have that the organization is secure and competent.

*Intellectual property risk*. Trade secrets or corporate strategy find their way outside the organization. Corporate espionage is increasingly common, with culprits launching attacks targeted to specific industries communication.
Identity breach risk: An organization fails to protect identity and other personal data belonging to customers and employees. The customer database maintained by the sales department is a high-value target. It goes without saying that customer financial or identity information is the most damaging asset to lose; it is possibly less obvious that the client database maintained by sales is also a severe loss.

Physical Risk: Theft or harm to assets or employees due to physical assets. This risk is most typically associated with physical theft but also applies to employee safety.

Regulatory risk: Encountering fines and other penalties for not properly handling different types of regulated information. Sarbanes-Oxley regulations are one example. In healthcare, privacy policies contained in HIPAA must be met or the company will risk penalties.

Corporate liability: A breach of security will cause harm to customers or suppliers for which the corporation will be liable. For example, if a payment database is compromised, the corporation may need to pay for identity insurance for its customers.

Availability risk: Information systems become unavailable which could halt work or, in the case of ecommerce systems, put the corporation out of business. Such an outage could be the result of a denial-of-services attack or of a natural calamity. The bulk of security controls are aimed at this risk.

Geo-political risk: A company’s information is valued by a nation-state capable of mounting and sustaining a formidable attack on information systems. Such attacks have been documented in several industries in the energy sector.

Knowing What to Protect
In summary, the outcome of the business analysis is an understanding of what the enterprise needs to protect. Note that this discussion does not mention specific technology components. It is a discussion best held with LOB leaders, rather than the IT organization. One result of these discussions might be the recognition that the company’s customer database has great value, letting the security team know that it must determine where the customer database is stored and how it is currently protected.

Performing Threat Analysis
Armed with an understanding of the state of the business, security planners are prepared to study the relationship between highly-valued information and the potential threats to that information. Rather than considering all systems and threats, the process is focused on threats to the organization’s most valued assets. These are the very assets that would most interest a hacker.

Where is that valuable customer database? Let’s suppose it is maintained and updated on a secure server inside the enterprise’s hardened core. Access to the database is restricted. So far so good. But what if the database is regularly replicated to many sales managers’ laptop computers? Driven by the business value of the customer database or the business risk of losing it, we’ve located a significant potential vulnerability.

It is at this point that a security professional is prepared to think through the possible solutions that best protect the customer database. One technical option is to encrypt replicas of databases on laptops, either by file encryption or by encrypting the hard drives of laptops that the replicas reside on. As an alternative, a process option might be implemented to disallow storing replicas
on laptops, such as allowing access to the data only by way of a virtual private network (VPN) that provides secure and authenticated access to the database on the server.

There will be no absolutely right solution for a typical threat. Different threats will emerge offering different levels of risk, cost, and impact on the business. Balancing risk, cost, and business efficiency is key to the strategic planning process. In a nutshell, important threats are the ones that put valuable business information at risk. They are threats to steal the riches of a company or to ruin the company.

**Adhering to Regulations**

Regulatory compliance presents itself as another category of business risk. Namely, the failure to comply can lead to penalties or even to sanctions that disallow a company from conducting some lines of business. Regulations such as those contained in the Sarbanes-Oxley Act in the United States prescribe criminal penalties for a company’s officers if corporate financial statements are found to be inaccurate.

The challenge for the security organization is to design controls that satisfy regulations and are, at the same time, sustainable and affordable.

Once again, the LOB leaders are the best source of information about the risk and the magnitude of impact of failure to comply with a regulation. Without LOB guidance, compliance quickly turns into a checklist activity with controls aligned with each regulation without regard to how the regulations align with the company’s business operations.

Strong security teams aim to achieve more than mere compliance with their adherence effort. They want to make sure that they implement the controls in a manner that minimizes the TCO and maximizes the value to the organization. This balancing act is referred to as sustainable compliance. Building out compliance programs that are both beneficial to the overall security posture and cost effective is a challenge for most organizations. In Chapter 6 of the book *Security Battleground: An Executive Field Manual* we discuss how to approach this challenge.

**Preparing The Strategic Plan**

At this point, we have identified business risks and regulatory requirements by working closely with LOB leaders. We have analyzed risks to understand the threats that would expose them. We have captured any changes in our business climate that affect regulation and compliance. We are now ready to step back and start the difficult decision process leading to prioritized security needs. In other words, we need to determine which security improvements we should invest in with our critical and limited resources.

It is important to note that this is not the time for resource allocation. It is merely the time for goal setting. Cost cannot be ignored but the objective for the strategic plan should not be confused with the budgeting process. The budget process and implementation plan will deliver on our strategic vision but they should not play a large role in defining it.

Once again, the strategic planning process for security should be the same as the strategic planning process for any other critical business function. A business does not decide to embark on a core initiative based on what it will cost. Instead, strategists first set a target and then analyze whether there is a viable way to achieve it. Budget and implementation planning come at a later step in the process.
So, how do we actually determine what needs to be done? To understand what we should target in our new strategic battle plan, we begin by reviewing our current security programs. The process is not that challenging because we maintained links between business risks, threats, and controls. For a key business risk that concerns us, we can focus on its associated threats. As we play this imaginary game of attack and defend, core deficiencies will come to light. For core deficiencies, we can now take a more traditional gap analysis approach. But the key here is that the gaps are now driven by our business demands and not by some security standard.

As we later defend our budget needs and process changes, identified business demands will enable us to be successful. Implementing a strong but disruptive control such as device management because it’s suggested by a standard will run a high likelihood of never getting deployed or funded. On the other hand, implementing a program to prevent the theft of design blueprints—if it is a key concern to an LOB leader—has a much higher likelihood of being funded and deployed to provide stronger protection to a valuable asset of the company.

**Maintaining the Strategic Plan**

The strategic planning process illustrated in Figure 1 provides guidance about the pathways from business risks to a security strategy. The plan will need to be revisited, although in many cases, not all components of the planning process need be involved. When tying the review of the plan to the annual budget cycle, it is important to keep in mind that changing events can accelerate the need for an updated strategy.

**Reviewing Business Risks**

For a stable business, the analysis of business risks (i.e., Riches, Ruins & Regulations) can be reviewed annually or every other year. Exceptions to this principle are triggered by significant changes in the enterprise. For example, if a company were to merge with or acquire another company, then a new business analysis will certainly be called for.

Other events that call for a fresh business review include significant shifts to new product lines, markets, regions, or countries. If, for example, an enterprise decides to enter the French marketplace, then the security team will need to review current practices in the light of French regulations and laws. Support for the new regulatory environment will be added to the security plan and to its budget.

**Refreshing the Threat Analysis**

The analysis of threats should be revisited more often—quarterly or perhaps twice a year. This analysis is not focused on maintaining existing security systems, but rather on understanding new threat vectors that have been reported. Once again, the foundation for the analysis remains the same: Are there new threat vectors directed at the enterprise’s riches or threatening its ruin?

It would be hard to argue for a refreshed threat analysis after every major news release by a security company. In reality, especially for smaller security organizations—a threat analysis cannot be an ongoing process. For a larger organization that can afford a full-time threat analyst, continuous monitoring is possible. The typical efficient security organization right-sizes the maintenance cycle to make it practical and sustainable.
**Reviewing Sustainable Compliance**

Even for a stable business, regulations will evolve. Typically, regulators and auditors can provide organizations with advanced warning about shifting compliance requirements and often with a timetable for satisfying the new requirements.

**Updating the Security Strategy**

The security strategy will need to evolve to reflect changes in the supporting elements. In our experience, the most frequent changes are driven by new threat vectors. For example, if we witness an outbreak in embedded attacks aimed at company copiers and printers, we may need to take a serious look at our business risks to see if this new threat vector could provide an easy exfiltration point.

The strategic plan should be reviewed to ensure that any new controls are optimized for added value to the overall security framework. In addition, controls that are in the organization should be routinely reviewed to ensure that they are providing as much value as possible. Doing this will improve the precision of budgets and ensure that the best TCO is in place for the next budget planning process. Average companies can recognize massive gains in security posture and reductions in TCO if they make strategic planning a core discipline that is rigorously executed.

**Lessons Learned**

- Security designed from the ground up to align with business risk will have the support, context and capabilities needed for success.
- The security-obligated executive must ensure that mitigating business risk is the solitary basis for new programs and critical investments.
- Technology-centric gap analysis cannot take the place of a real strategic plan.
- A business-centric understanding of what needs protection should permeate all aspects of the security delivery and planning process.
- A security-obligated executive should expect a strategic plan that explicitly shows how levels of protection are proportional to the impact (i.e., cost) of a security breach.
To gain additional practical advice oriented for security-obligated executives, please refer to the book *Security Battleground: An Executive Field Manual* by Michael Fey, Brian Kenyon, Kevin Reardon, Bradon Rogers and Charles Ross.

**About the Authors**

**Michael Fey** is Senior Vice President of Advanced Technology and Field Engineering at McAfee, responsible for leading McAfee’s worldwide technical go-to-market strategy. In this role he leads a global organization responsible for collaborating with customers and prospects to define, design, and implement strategic security technologies. Michael also provides oversight of new acquisitions for the McAfee corporate market segment. Before McAfee, he held multiple technical management positions at Opsware and Mercury Interactive.

**Brian Kenyon** is Senior Director of Solution Architecture at McAfee, where he is responsible for leading an engineering organization focused on developing comprehensive security and compliance. Prior to McAfee, Brian was chief architect at Foundstone and was instrumental in designing and developing the company’s solutions and product service line. Brian is lead author of Security Sage’s Guide to Hardening the Network Infrastructure, and contributing author of network architecture for Special Ops: Network and Host Security for Microsoft, Oracle, and UNIX.

**Kevin T. Reardon** is the Senior Director of Worldwide Value Consulting for McAfee. During his 17 years in the IT security field, he has worked with product delivery and implementation teams at McAfee and was vice president of operations and compliance strategy at Preventsys. An expert on policy frameworks for a variety of industries and sectors, Kevin has advised numerous Fortune 500 companies on designing and implementing programs, strategies, and training for security systems and processes. He has also contributed to several key publications on the topic of Microsoft Windows security.

**Bradon Rogers** is Vice President of Worldwide Technical Operations at McAfee. In this role, Bradon is responsible for worldwide operations for the McAfee global field engineering organization. Prior to joining McAfee, he managed the worldwide field engineering team at Secure Computing prior to its acquisition by McAfee in 2008. Before Secure Computing, he joined the founding team of security startup, CipherTrust, where he managed the field engineering team and was engaged in corporate strategy, field technical sales, strategic customer engagement, and security threat research. He also held various field and product engineering roles at Oracle, Lancope, and Group 8760 before joining CipherTrust.

**Charles Ross** is the Vice President of North America Technical Operations at McAfee and plays a key role in assisting customers and partners with security strategies that will help them achieve their critical security and business initiatives. Prior to McAfee, Charles served as security consultant for Deloitte & Touche, consulting with Fortune 500 companies to assess, develop, and implement world-class security programs. Charles is a frequent speaker on security topics and holds multiple patents in the areas of information security assessment and optimization.