Key Components of a Risk-Based Security Plan
How to Create a Plan That Works

Authors:

Vivek Chudgar
Principal Consultant
Foundstone Professional Services

Jason Bevis
Director
Foundstone Professional Services
Key Components of a Risk-Based Security Plan

As management is increasingly involved in information security budgets, many questions are being asked – Did we really need to spend this money or could we have done without it? Are we really more secure now than before? Would we be more secure if we installed this product or spent money on security training? While these questions are obvious, answers are not. A smart CSO or CISO would anticipate these questions and should be prepared with the answers even before the question is asked. This paper takes a pragmatic view of the different components of an effective security plan, and provides a perspective on how enterprises serious about their information security budgets should think about their security plan. It describes the approach to identify the components of the security plan before a full-scale plan is developed and helps answer the questions above with confidence and ease. Enterprises that adopt this approach will also reap other benefits such as higher credibility and acceptance for the security programs, as well as optimum ROI with a measurable increase in the overall information security posture.

Introduction
Information security has long been considered a secondary IT function. As a result, information security budgeting has been minimal and often misallocated solely as a part of the general IT budget. CISOs and CSOs obviously want to change this. In many cases, they would like to see an information security organization separate from the IT organization, as well as a separate budget for their information security needs.

Opportunity for CSO/CISO
Strict enforcement of information security-related regulations and compliance requirements have caught the attention of executive management and provided CSOs and CISOs with an opportunity to make a case for a separate information security team and budget. Before approving such an organizational and budgetary change, the management is bound to ask tough questions and demand clear answers. They are also likely to ask for a long term strategy that convincingly addresses the core security challenges faced by the enterprise instead of simply tackling the day-to-day tactical security issues.

Ideally the CSO/CISO would present a security plan along with a security budget that can easily answer these questions and win the approval of the executive management. Unfortunately, security budgets based on a traditional approach fall short on many counts. Therefore, it is likely that such a budget won’t be able to withstand the scrutiny of the executive management, and as a result, fail to gain the necessary approvals. In many cases, the result is that a separate compliance program is set up, which inadequately addresses security as a whole and provides a false sense of security.
Traditional Security Budget Doesn’t Impress the Executives

Let’s better understand why a traditional security budget won’t impress executives. The traditional approach has been to develop an IT security budget based on the results of a vulnerability assessment. Typically the goal of vulnerability assessments is to test the critical IT systems and applications and identify exploitable vulnerabilities. The result usually is a large list of vulnerabilities along with appropriate recommendations to address all vulnerabilities. The security plan/budget is then drawn up to implement these recommendations.

Vulnerability assessments are highly technical and focused on a few critical systems and applications. Therefore the vulnerabilities identified by such assessments are primarily related to Technology. Vulnerability assessments unfortunately do not do a good job of identifying vulnerabilities related to People and Processes. For example, suppose only two low-risk vulnerabilities were identified in a system being tested at one point in time. Assume that after three months these two vulnerabilities were not patched and suddenly became critical due to an active exploit being released. At this point the problem is no longer just a technology issue, but more likely a problem in the patch process or lack of resource to implement the process.

Another weakness of vulnerability assessments is that the tests are tactical in nature and unfortunately miss out on the larger strategic picture. The server holding the sensitive customer data may be secure, but what if the desktop used by the customer relationship executives to access the customer data is vulnerable?

Therefore, a budget drawn up based on results of a vulnerability assessment can only cover short-term tactical requirements and a few strategic requirements that address Technology needs. Critical and mostly strategic vulnerabilities related to People and Process as well as some Technology areas will be overlooked.

A tactical budget will not be enough for several reasons:

1. First, as expected, the executive management’s knowledge of technical aspects of information security is rather limited.
2. Second, the executive management knows that tactical expenditure without a strategic direction is like a boat without a sail – it will take you somewhere, but it may not be where you wanted to go. As a result, a tactical budget will most likely not gain their approval.

What Will Impress the Executives?

This paper presents an effective approach to address this situation: a Risk-Based Security Plan. The graph below summarizes the different stages of a risk-based security plan.
**Key Components of a Risk-Based Security Plan**

*Step 1 - Information Security Risk Assessment:* It all starts with an information security risk assessment based on industry standards. An information security risk assessment identifies, measures, and prioritizes the risks based on several factors such as impact, likelihood, affected IT assets, etc. Once the risks are identified, appropriate recommendations (strategic as well as tactical) are drawn up to effectively address these risks.

*Step 2 - Security Plan:* The security roadmap recommendations as well as the overall strategic, tactical, and operational goals of the organization serve as the input to the security plan. The security plan translates these recommendations (prioritized by risk and overall organizational goals) into actionable activities, outlining the specific projects needed to address these recommendations, resource requirements for each project, and suggested timelines.

*Step 3 - Security Budget:* Once the information from Step 2 is available, drawing up an information security budget is relatively straightforward and effortless. The resulting budget will:

- Clearly reflect the strategic direction taken by the information security team
- Identify the underlying risks being addressed by each budget line item
- Identify IT assets that will benefit from the project
- Provide an opportunity to measure the overall improvement in the risk posture of each IT asset

For those familiar with the ISO/IEC 27001¹ standard, it is easy to notice that this approach aligns very well with the approach suggested by the ISO/IEC 27001 standard to implement an information security management system.

Let us look at each phase with examples.

**Getting Started: Risk Assessment**

Information Security Risk, like all business risk, can be managed in order to operate within a threshold that is appropriate to the business conditions or regulatory requirements. In order to manage risk, companies must first understand the risk residual in their organization by conducting a risk assessment.

Several industry standards exist that provide a formal and repeatable structure to risk assessments, e.g. SP800-30 (Risk Management Guide for Information Technology Systems) by NIST, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) by Carnegie-Mellon University’s Software Engineering Institute, etc. These standards help ensure that the results of each risk assessment are repeatable and comparable, as well as dependable.

---

¹ ISO/IEC 27001 - Information technology — Security techniques — Information security management systems — Requirements
This section describes Foundstone Professional Services’ approach to performing a risk assessment and sets the context for developing a risk-based security plan. The key phases of a risk assessment are:

<table>
<thead>
<tr>
<th>NIST SP800-30 Methodology</th>
<th>Foundstone Risk Assessment Methodology</th>
</tr>
</thead>
</table>
| 1. System Characterization | 1. Information Gathering  
Thoroughly understand the business  
2. Asset Identification  
Rank mission critical assets that support the business operations based on criticality |
| 2. Threat Identification | 3. Threat Identification  
Rank the threats that can affect critical assets |
| 3. Vulnerability Identification | 4. Vulnerability Identification  
Identify the severity of vulnerabilities in critical assets |
Identify mitigating controls in place for each critical asset |
| 5. Likelihood Determination | 3. Threat Identification  
4. Vulnerability Identification  
Determine likelihood of vulnerabilities being exploited |
| 6. Impact Analysis | 5. Risk Analysis  
Prioritize risk by focusing on assets affected by credible threats and existing vulnerabilities |
| 7. Risk Determination | 5. Risk Analysis  
Create a risk matrix to capture information from previous steps |
Determine security strategies that minimize risk and maximize ROI |
| 9. Results Documentation | 7. Deliverables  
Develop deliverables, including roadmap and executive summary |

**Information Gathering**

During the information gathering phase of the engagement, the focus is on identifying the three key risk components: *assets, threats, and vulnerabilities*. The Foundstone approach is asset-centric, meaning the risk assessments begin with...
the identification of the environment’s assets that are central to business operations. The information gathering phase consists of individual interviews with department managers and technical staff, reviews of documentation relating to information security, and an examination of the assets that will be identified.

**Asset Identification**

As the goal of a risk assessment is to identify the risk to critical business operations, the first step in the risk assessment is to identify the assets that support critical business operations. These assets may include physical and logical assets such as physical facilities, employee computers, network communications devices, operating systems, and applications. Interviews, workshops, architecture diagram reviews, and disaster recovery plan reviews can help determine the important assets in the environment. The assets should then be ranked based on their criticality, confidentiality, or both, depending on the goals of the organization. As an example, consider the two asset ranking models below, where the number 4 represents the highest rank.

<table>
<thead>
<tr>
<th>Criticality Ranking</th>
<th>Confidentiality Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 = Catastrophic</td>
<td>4 = High Risk Data</td>
</tr>
<tr>
<td>3 = Critical</td>
<td>3 = Confidential Data</td>
</tr>
<tr>
<td>2 = Marginal</td>
<td>2 = Internal Data</td>
</tr>
<tr>
<td>1 = Nominal</td>
<td>1 = Public Data</td>
</tr>
</tbody>
</table>

**Threat Identification**

Threats are individuals, groups, or external events such as environmental factors that can negatively impact assets. Threats can take many forms, including people (such as insiders or Internet users), technology (such as worms or Trojans), and events (such as floods or fires).

Examples of impacts produced by threats include:

- Affects to confidentiality
- Affects to integrity
- Affects to availability
- Direct costs from physical destruction/loss
- Direct costs from theft or extortion
- Costs to resolve incidents (internal productivity loss, outside resources)
- Loss of consumer confidence
- Failure to meet regulatory requirements
- Failure to meet contractual agreements
- Worst case scenarios (catastrophic failures of information systems that result in physical destruction, death, injury, or inability to continue operations)
The threat scenarios can only happen if a threat impacts an asset that has a real vulnerability. However, understanding how the threats might impact your enterprise assets is an important step in the risk assessment process. For example, a threat of a category 4 hurricane may be high, but if your enterprise facilities are built to withstand a category 5 hurricane then the there is no real vulnerability or impact to the facility. Therefore, the output of this stage of the assessment process is a ranking of threats based on their prevalence. Prevalence is a measure used to indicate if a particular threat has the capability and motivation to impact each asset.

It is important to understand that capability and motivation are important attributes for threats that involve people (e.g. cyber threats, corporate espionage, etc.), and these threats need both attributes to be credible. For example, consider the scenario when the threat is an Internet-based attacker and the asset is a cash management system connected to the Internet. The attacker has motivation in the form of monetary gain and capability via hacking skills. Therefore each identified asset must be analyzed based on the threats that have the ability to affect them, and each threat must be ranked based on prevalence.

Once the results of threat analysis are recorded, it is possible to review the asset and threat information collected to determine possible impacts to data. However, the likelihood of these impacts cannot be determined without the final component of the risk assessment, which is the vulnerability assessment.

**Vulnerability Identification**

Threats cannot impact assets unless the assets are vulnerable to those threats. For many of the possible threats, mitigating controls may be in place to reduce the likelihood of a threat exploiting a given asset. Thus, understanding the unmitigated threats (vulnerabilities) that exist on critical assets is a key step in the risk assessment.

Vulnerabilities that affect critical assets are typically identified through interviews, documentation review, and a technical analysis (e.g. vulnerability scans or penetration testing). Vulnerabilities are then classified based on their severity, where severity identifies the exposure of an asset.

Any protective measures in place for each asset must be considered before determining the potential for a threat to be exploited. Comprehensive information security programs require that every asset have protective measures in the areas of prevention, detection, and response:

- Preventative measures reduce the likelihood of exploitation.
- The ability to detect and respond to incidents allows an organization to minimize loss in the event of a compromise.
- Finally, effective detection and response provide a deterrent to exploitation attempts.

**Risk Analysis**

The result of the information gathering phase is a collection of data that represents the assets critical to operations, the threats that may impact those assets, and the vulnerabilities associated with those assets. Risk is present when critical assets, credible threats, and existing vulnerabilities coincide.

As the goal of the risk assessment is to identify and prioritize risk to guide the formulation of security strategies, Foundstone Professional Services recommends a qualitative risk assessment rather than attempting to assign monetary...
values to potential losses. Foundstone recommends this approach because of the limited data available on likelihood and costs and the difficulty in accounting for liabilities, e.g. the loss of consumer confidence.

This approach is also supported by the General Accounting Office/Accounting and Information Management Division (GAO/AIMD-00-33) Information Security Risk Assessment report and is considered advantageous according to NIST 800-30.

**GAO/AIMD-00-33**

“It is important that organizations identify and employ methods that effectively achieve the benefits of a risk assessment while avoiding costly attempts to develop seemingly precise results that are of questionable reliability.”

**NIST SP800-30**

“In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.”

After determining the risk associated with each asset, the assets can be ranked based on their risk values. This relative risk ranking should be the focus of further analysis, as opposed to the specific numeric values assigned to each asset.

---

**Develop Security Roadmap**

After ascertaining risk within the environment, the next step is to develop strategies to manage that risk. Risk exists due to the confluence of assets, threats, and vulnerabilities, and accordingly mitigating controls which reduce one or all of
these factors will reduce the overall risk to the organization. At this stage, it is critical to focus on strategies that maximize return on investment, as well as consider other relevant factors such as their effectiveness in your environment, legislative requirements, organizational policy, operations, safety, reliability, etc.

The security roadmap should clearly represent the risks faced by the organization and risk management strategies that can be employed to reduce those risks. Risk management strategies fall into four categories:

- **Risk Mitigation**: In Foundstone’s experience, the majority of current security risk management is mitigation – reducing the exposure through security countermeasures (people, process, and technology).
- **Risk Transfer**: If you are outsourcing IT or security functions, can you transfer risk (contractually) to a third party, or can you transfer risk to an insurance provider?
- **Risk Avoidance**: Can you avoid any existing risk, such as by eliminating an existing online or network capability?
- **Risk Acceptance**: Some risk will be cheaper to accept than fix. There is definitely a point of diminishing returns with security spending.

Risk mitigation remains the most common security risk management strategy because much of the risk associated with security cannot be transferred or avoided – it must be reduced. For example, you cannot truly transfer the risk associated with a defaced web page or publicly release customer data because the potential loss is virtually impossible to predict.

**Defining the Future Environment**

Creating the security plan begins by focusing on the strategic, tactical, and operational goals to define a desired future security posture. The long-term future environment is always a moving target, so the plan must be set up to be dynamic so it can be adjusted as needed. This security posture must also be realistic and ensure return on investment is consistent with business objectives and not to the point of diminishing returns. With this approach, the goals and the risk assessment recommendations can be prioritized in a phased manner over a period of time. The outcome will be a plan with short-term activities looking out a period of three to six months, midterm activities that will be completed in six months to two years, and long-term activities that will complete the future environment within a three to five year period. This approach will provide clear direction to management and an understanding as to why the budget is necessary.

**Identifying the Gaps**

Once the risk assessment is complete and the future security posture is determined, the next logical step is to identify the gaps of the current organizational environment and the future environment. This will help with additional prioritization of activities. For example, there may be vulnerabilities associated with a high risk asset; however that asset is being replaced in Phase 2 of the future environment. As a result, minimal efforts may be put into place because the asset is going to be
Key Components of a Risk-Based Security Plan

decommissioned. The plan should reflect this organizational goal and prioritize mitigation factors correctly. This can be done by outlining all of the gaps between the current and future environments and then aligning the risk recommendations accordingly.

**Developing the Plan**

The resulting plan as mentioned above should be a multi-phased plan spanning three to five years including all the defined projects and their associated activities defined during this entire process. It is important that the plan be divided into sections based on audience. This will help ensure the plan can be communicated in part or in its entirety for the particular audience. The plan is a mechanism to provide management a quick summary supporting the need for security, providing insight into all vulnerabilities identified in the risk assessment, the activities to remediate them, and the budget for each activity. The plan is also a mechanism to provide the detailed activities, timelines, and responsibilities for implementation to each particular audience. For instance, the high-level timeline below provides an overview of two possible sections of the plan. Both are tailored to an audience – one being the staff performing risk assessments and the second being the development staff.

<table>
<thead>
<tr>
<th>Plan Section and Activities</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Develop a Formal Risk Assessment Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Conduct Ongoing Enterprise Risk Assessments</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Re-evaluate Open Risk Items</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Revise Asset Management Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Software Development:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Develop Secure Coding Guidelines</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Enhance Software Development Lifecycle</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In addition, to the above plan sections, a plan should address the following areas:

- Executive Summary
- Security planning and Governance
- Security Policy
- Network and Systems Security
- Business Continuity Planning
- Personnel Security
- Audit and Compliance
- Physical Security
Ready for Management: Information Security Budget

With all this detail and supporting information in the security plan, it will be much easier to address management’s concerns and make a convincing case for increasing the security program budget. A clearly presented summary with a budget aligned to each task will provide management the information needed to make the correct decisions.

With detailed activities in front of us, a budget can be drawn up with relative ease based on man-hour estimates for each activity. A fair estimate of the hourly rate for internal employees coupled with associated hardware/software costs will provide the approximate dollar amount required for each activity.

<table>
<thead>
<tr>
<th>#</th>
<th>Title</th>
<th>Description</th>
<th>Phase</th>
<th>Level of Effort (hours)</th>
<th>Labor Cost</th>
<th>H/W, S/W Costs</th>
<th>Estimated Project Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Develop Secure Coding Guidelines</td>
<td>Revise the coding standards for all critical ASP.NET software platforms.</td>
<td>1</td>
<td>200</td>
<td>20,000</td>
<td>N/A</td>
<td>$20,000.00</td>
</tr>
<tr>
<td>2</td>
<td>Enhance Software Development Life Cycle</td>
<td>Revise the software development lifecycle process to include secure development best-practices during the design and testing stages</td>
<td>2</td>
<td>240</td>
<td>24,000</td>
<td>N/A</td>
<td>$24,000.00</td>
</tr>
</tbody>
</table>

Armed with these details, the CISO/CSO can easily answer management’s questions when they ask: “Did we really need to spend this money?” The detailed security plan will enable the management to look at each vulnerability identified during the risk assessment as well as the activities in the plan, and decide to mitigate, transfer, avoid, or accept the risk.

The next question “Do we have enough resources?” becomes evident immediately and can be adjusted based on the expected plan implementation timeline. For instance, notice in the example above it takes 200 hours to develop secure coding guidelines and the labor cost is $20,000. This is based on a $100/hour internal rate for an employee. If the rate was different for sub-contractors or outsourced staff, each item would be adjusted accordingly. Also by providing the estimated hours for each task, the resources required for performing each activity becomes apparent. In this case, if the project needs to be completed in three weeks, it would require two resources; otherwise it could be done in five weeks with one resource.

Finally, an easy-to-understand budget provides everything in a presentable format to management. This is accomplished through the security plan executive summary, which is tailored for that particular audience and focuses on the need for security, the timeline for each activity, and the budget to remediate the vulnerabilities identified in the risk assessment.

Summary

The key to getting the appropriate budget and making this a reality is for the CISO/CSO to acknowledge the need for a strategic approach to information security. Once this need is acknowledged, the next steps for the CISO/CSO are to anticipate management’s questions, plan ahead, and be ready with an explanation of what strategic security issues will be addressed by each dollar of the security budget. A well-researched and well-prepared security plan along with a well-presented security budget cannot fail the CISO/CSO on a mission to get the precious resources needed to address the security issues.
About Foundstone Professional Services

Foundstone Professional Services, a division of McAfee, Inc., offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company’s professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.

Foundstone understands the drivers for risk assessment, the strategic importance to the organization, and the challenges of risk management. Due to our unique assessment, incident response, and forensics experience, we understand the vulnerabilities and potential for loss unique to information technology.

Foundstone’s risk assessment methodology provides the framework for ongoing risk assessments and updates by its clients. The matrices, questionnaires, and process that we use are clearly documented and provided to our clients during the risk assessment. Updates and future risk assessments can be performed on a recurring basis without outside assistance, if desired.

Foundstone’s communication skills – both written and verbal – are another key differentiator. Many regulatory requirements mandate a report be submitted to various agencies, such as the OMB, directors at various agencies, and congressional committees. Foundstone’s reports and consultants enable senior level management to rapidly and effectively understand the information security risks facing the organization and meet regulatory reporting requirements.