Security Assessment Methodology

A White Paper from Vigilinx

Vigilinx
Digital Security Solutions

Table of Contents

Any inquiries should be addressed to:
info@vigilinx.com

www.Vigilinx.com

Executive Summary

Security Assessment Methodology

Making It Useful to the Organization

Organizations have many options for assessing their security. However, unless their management clearly understands the motivations and methodologies of potential vendors, a security assessment will confuse matters rather than make them better. By understanding the assessment process, organizations can make a more informed choice of assessment vendors.

This White Paper explores the major components of a security assessment and how the offers of various security-consulting vendors differ. It explores issues of standardization, industry practice, organizational models, and risk measures. By combining these using a well-designed assessment methodology guided by a quality assessment tool, organizations can maximize the value they receive from a security assessment.

Introduction

Security remains the leading concern senior executives have about their information and network infrastructures. In many cases, it is not clear whether the range of security technology in use affords the protections the organization requires. Even more disconcerting, many security solutions seem to disrupt normal operations. Employees see slow or blocked access to e-mail, critical applications, and other internal resources. Virtual private networks (VPNs), firewalls, and e-mail gateways confound interactions with customers, vendors, and business partners.

More and more, executives ask, "Do we really need all this security? How do we know where we really stand? Can somebody give me a gauge that lets me know how we're doing with respect to our peers? What's the priority for security in our organization?"

Getting Answers

Traditionally, organizations have taken two approaches to answering these questions:

- Assigning the evaluation of security measures and their requirements to an internal committee (often, a committee of one) to study the problem and report back to senior management, or
- Hiring an outside organization, such as the corporate auditor, to perform the study and deliver a formal report.

Creating an internal committee is attractive because it keeps the problems "inside the family." Very often, more than one skeleton lurks in the closet, so the smaller the community of people that knows about private issues the better.

However, the committee has several uphill battles to fight. First, it may not have the in-depth expertise to evaluate security measures. As a result, it can never assure its members, or management, that it has addressed all important criteria. Second, the time constraints of members' other duties make it difficult for them to complete the study in a timely manner, unless they neglect other critical business imperatives. Finally, because the committee members are part of the organization, they can never achieve true objectivity. Friendships and office politics may block the way for an impartial result.

Hiring an outside organization is the approach often taken by larger companies. Originally, when information technology was less mature than it is today, there were few places to turn for this help. Most obvious was the corporate financial auditing firm. The "Big 5" (or their predecessors) tried to develop specialties in information security. A few technology companies, most notably system and network integrators, also began to offer such services.

In both cases, however, these organizations perform "security assessments" as a sideline. They remain most capable in their core competencies: business consulting or technology sales and service, respectively.

More recently, a new option has developed: specialty security firms which have built dedicated teams of highly skilled experts in the technologies and processes of security. Increasingly, this segment of the industry is becoming the obvious choice for getting answers to security questions.

Cost is Still a Factor

Retaining an outside organization for a security assessment costs real money. Most vendors quote prices starting in six figures for a "comprehensive" engagement. More importantly, they are often vague about what they will and won't include as part of the scope. Unless they are truly huge, most companies probably haven't budgeted for such an expense. People seldom have security at the front of their minds when they carve up the limited funds at the beginning of a fiscal year.

Price Ranges for Security Assessments

Vendor	Low Price	High Price
"Big 5" Auditors	$0*	$1,000,000
Integrators	$0*	$150,000
Security Boutiques	$40,000	$250,000

* Most auditing firms and integrators offer "come-on" assessments for free in order to identify significant follow-on tasking.

An integrator may offer a "free" security review as an incentive for a large deployment contract. Big 5 auditors may "bury" the cost in an annual audit fee. Some security boutiques bill their penetration testing services as a complete solution.

In the final analysis, it is impossible to compare these costs to each other. All provide limited scope. In most cases, a "free" assessment is worth what you pay for it. Business audits rarely provide the detail necessary. (And, since Big 5 partners do understand how to profitably price their projects, you're *not* getting a deal.) Penetration tests can only explore about a third of the technology issues of security and completely pass over processes and people.

Settling on a Standard for Completeness

Fortunately, various security-conscious standards organizations – such as the British Standards Institute (BSI), International Standards Organization (ISO), the U.S. National Institute of Standards and Technology (NIST), and the International System Security Association (ISSA®) – have undertaken the task of standardizing what we mean by security. The first of these, BSI, developed BS 7799, which was adopted by ISO as ISO 17799. This standard creates a veritable "laundry list" of security criteria, laying the foundation for a comprehensive assessment of any organization. There are other standards from these and other organizations, but BS 7799 (ISO 17799) has become the most widely accepted and recognized.

Because so many security standards exist, it is often difficult to determine which best applies to an organization. Generic standards offer the most comprehensive view, but these often require security measures that are inappropriate in one or another industry. They fail to take into account the context.

For example, the concept of intellectual capital is relatively unimportant in newspaper publishing, since news is printed within hours of its gathering. A law firm, on the other hand, must keep close wraps on the information it uses, to protect the privacy of its customers, while a biotech firm must protect its trade secrets.

Security-Related Standards and Regulations

- ISO 15504 (Common Criteria) – ISO
- CobiT – IT Governance Institute
- ISO 17799 (BS 7799) – ISO/BSI
- X.800 (formerly ISO 7498-2) – ISO
- HIPAA – U.S. Congress

The best assessments adapt standards to the type of organization they evaluate. This is sometimes possible by using industry-specific standards, but these documents frequently do not cover the breadth of issues that the generic standards do. More importantly, few industries have actually adopted standards, although the number is steadily growing. To ensure good agreement with industry practice, the auditor should possess industry benchmark data on security practices for a wide variety of market segments.

Making It Relevant

Unfortunately, the nature of standards documents often makes them rather difficult to comprehend as a whole. Experienced security experts can traverse the list of criteria, but the assessment customer usually lacks the training and experience to make the standard relevant to its business situation. Just as a shopping list doesn't guide you through the grocery store, the security standard doesn't guide its application and interpretation.

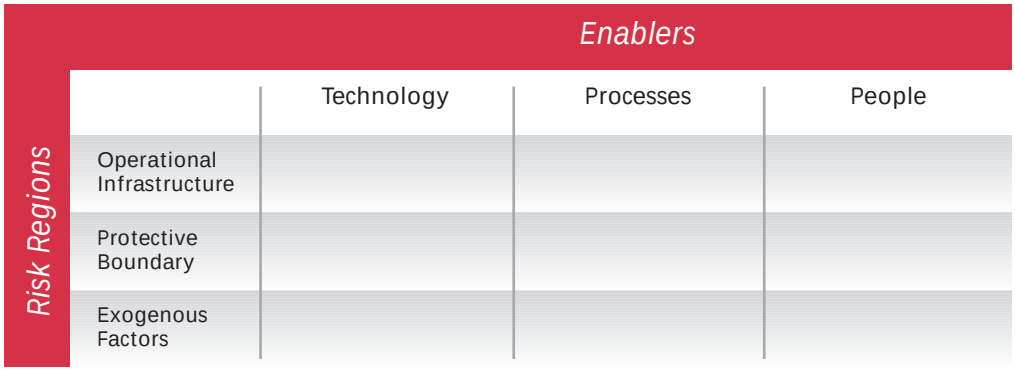
What is needed is a map that makes it easy to interpret the assessment findings in the context of the organization. Serving as a model of the organization, the map routes readers through the results. Making the findings relevant greatly enhances their value to the customer.

The most obvious way to model an organization is to partition it into "risk domains." For many e-business applications, three major "risk domains" will suffice: *Operational Infrastructure, Exogenous Factors, and Protective Boundary.*

- *Operational Infrastructure* includes the systems and information vital to the organization's ongoing business. These are usually the "crown jewels" that require the highest level of protection. Most often, there are compartments (sub-domains) within this domain. For example, most companies have human resources records, financial data, executive information systems, and intellectual capital that must be kept safe from outsiders. Moreover, these sub-domains must not intermix. As a result, issues of employee privacy, insider trading, and tactical and competitive advantage dictate that the business apply appropriate best practices to securing the *Operational Infrastructure.*

- *Exogenous Factors* reflect the environment in which the organization must operate. They include customers, partners, vendors, and regulatory agencies. Exogenous Factors also include hackers and other nefarious individuals or groups that would do harm if given a chance.
- The *Protective Boundary* enforces the division of the first two domains. It keeps in that which must stay in, and keeps out that which must stay out. But, when appropriate, the *Protective Boundary* should enable free exchange of services and data.

Security Assessment Scoring Matrix



After completing a meaningful security assessment, organizations should have an objectively scored, holistic view of their security posture as represented in the Security Assessment Scoring Matrix above.

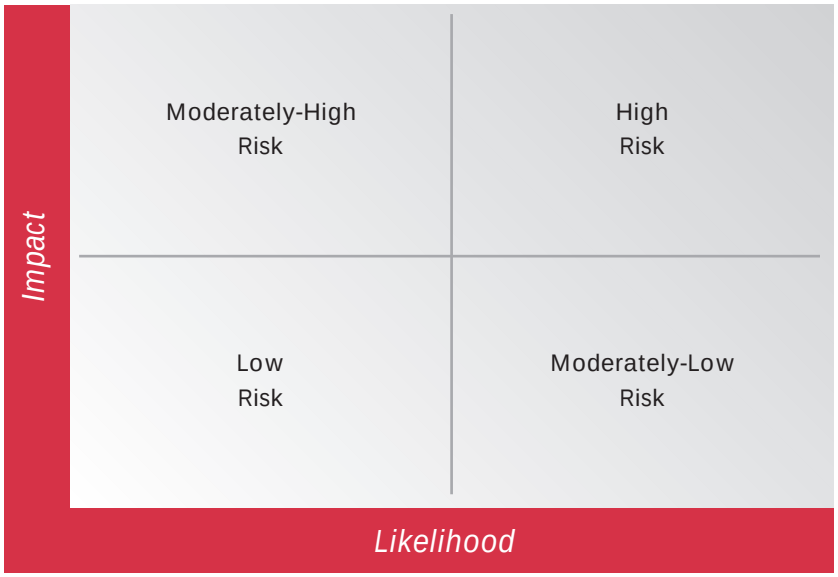
Within the risk domains there are enablers, which act to secure the domain. Conventionally, security experts divide enablers into *Technology, Processes*, and *People.*

Most organizations pay careful attention the first of these, using firewalls, access control mechanisms, authentication servers, virus scanners, intrusion detection systems, and a plethora of other devices and software. However, *Technology* enablers are ineffective without careful attention to the *Processes* which operate and maintain them. Moreover, *Technology* can be cost-prohibitive to apply across-the-board. In some cases, *no* mechanism exists to fill a particular void. This is where *Processes* and *People* become even more important.

Putting the risk domains together with the enablers leads to a simple, 3-by-3 matrix that is easy to comprehend. It permits assessment consultants to present their findings to customers in a way they can understand, framing the security criteria in the context of the business.

How to Measure the Benefit

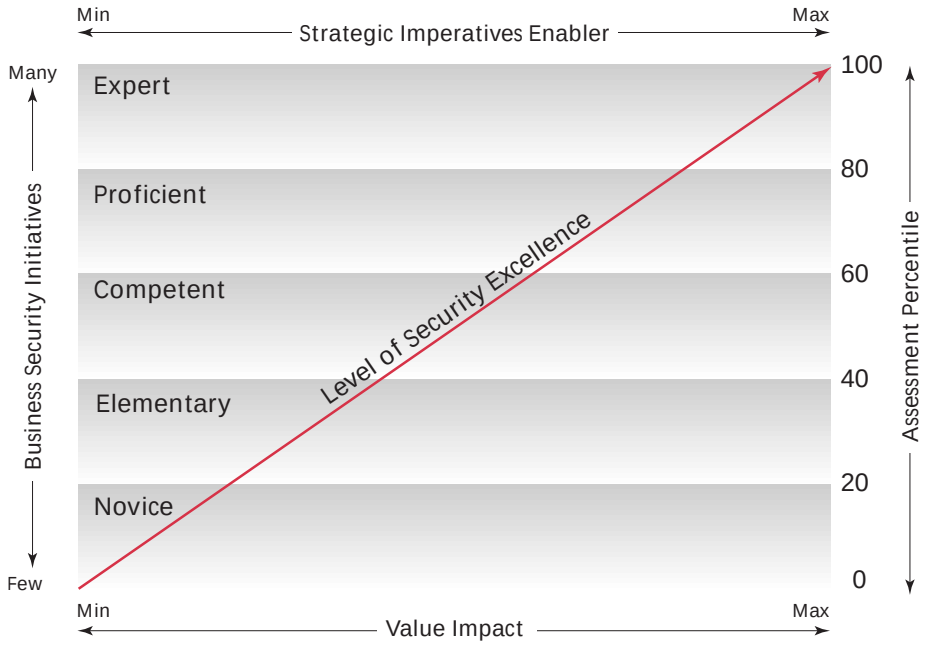
While standardizing the criteria (and doing so comprehensively) is necessary, it is not sufficient to guarantee a quality assessment. The critical objective of any assessment is to determine the most cost-effective manner to reduce residual risk to an acceptable level. Failure to meet this objective renders the project's output worthless.



Two components comprise risk: impact and likelihood. For example, penetration testing can gauge an Internet connection's likelihood of breach. However, even if the testing reveals major vulnerabilities, it still provides no basis for determining risk. That's possible only by understanding what, if any, impact such a breach would have on the organization. Low impact greatly reduces the risk such vulnerability poses. Conversely, exposure of a sensitive data repository – customer credit card numbers, for example – represents a high-impact incident. Any known vulnerability affecting that repository leads to a high risk.

Cost is the other major factor that makes the results of a security assessment relevant. Executives need to prioritize risk remediation activities. Setting these priorities depends, largely, on the cost/benefit tradeoff.

In this case, reducing risk is the benefit, so cost is the independent variable. Cost, in turn, has its components. For example, the capital cost of security technology represents a real dollar value that anybody can understand. Similarly, the labor expense to implement and integrate the technology is easily measured. Ongoing maintenance, which is often overlooked, must factor into the equation, too.



However, the most difficult cost component to estimate is the level of disturbance the security measures will have upon normal business operations. Everyone has experienced that "got-to-have-it, whiz-bang" software feature that slowed the network to a crawl. Security controls, by design, are intended to impede information flow. This intent only serves to magnify the "whiz-bang" effect. Once in place, security technology often takes on a life of its own, requiring staffing for fulfillment and troubleshooting. Yet, even the best-operated security solution can cause problems in unpredicted ways.

Experience Bridges the Gap

Standards define the spectrum of security controls that can be put into place. They also establish criteria for measuring those controls. However, determining the risk that the controls affect, and the benefit to the organization, requires experience and knowledge.

Security technology vendors often claim maximal effectiveness for their products, but in practice, achieving many of these benefits results in reduced functionality or performance in other areas. Thus, the technology's practical effectiveness is much less than claimed. Only hands-on experience can provide this kind of insight.

Similarly, password policies seem to ensure that the odds a hacker can guess right are very slim. Realistically, though, users will disobey password policies, often creating trivial passwords that are the entrée for the motivated attacker, unless they understand these policies' value to the organization. Again, only experience with organizational behavior enables an assessment consultant to identify the deficiency and recommend appropriate training and awareness programs.

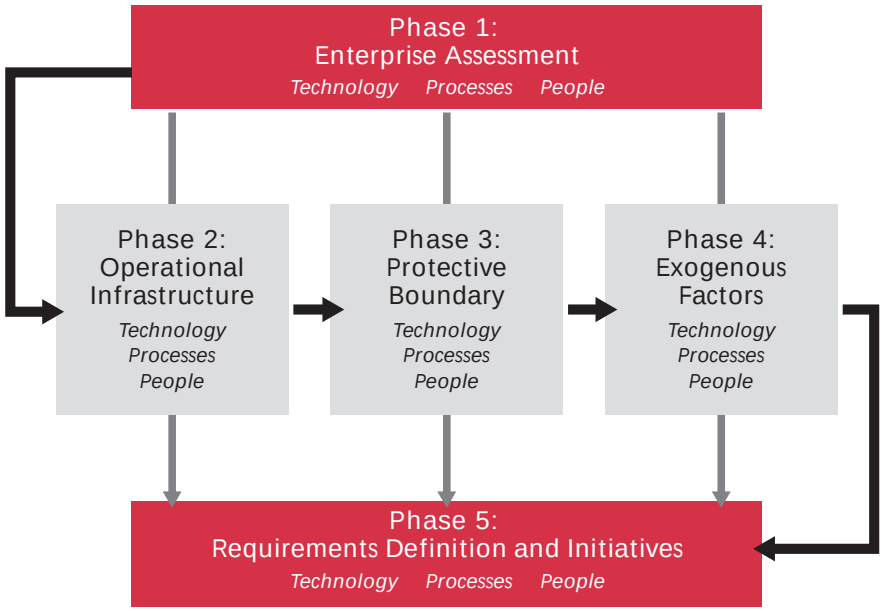
Administering a security assessment as a simple questionnaire overlooks the value of experience. Such mechanical processes can only go so far toward ensuring an organization's security posture. Uncovering subtleties, and getting past claimed capabilities to reality, requires the personal touch. Only an experienced advisor can make cost-effective recommendations with respect to *technology*, *processes*, and *people*.

The VBSA™ Approach

Vigilinx has developed its business security assessment (VBSA™) to offer a cost-effective way to measure an organization's security program within the business context. It leverages the decades of experience of Vigilinx senior staff with assessing and developing these programs. This experience is captured within a proprietary tool for use by knowledgeable Vigilinx security experts.

The tool affords four big wins for the security assessment customer:

1. It ensures comprehensive coverage of all security issues by tracking an enhanced set of standard security criteria.
2. It emphasizes relevance of the results to the organization by using an organizational model.
3. It considers the organization against appropriate security best practices for its industry.
4. It minimizes assessment costs by enforcing a structured methodology.



Vigilinx has used the most popular security standards to guide consultants through the security assessment process. While it tracks the standards, the tool enforces a structured approach to explore *technology*, *processes*, and *people* issues within each risk domain. The VBSA methodology proceeds through five phases including *Operational Infrastructure*, *Protective Boundary*, and *Exogenous Factors*. This methodology maps directly to specific groups of security criteria within the tool. Each criterion is associated with a set of guiding questions to expedite the job of exploring how the subject organization meets it and whether or not it represents significant risk.

Completion of all five phases provides Vigilinx the information it needs to produce the final report, which consists of three major components:

1. Security Findings: A list of security deficiencies that increase risk to the organization.
2. Recommendations: A prioritized set of activities and security programs to address the findings. Vigilinx computes priorities by ranking the relative cost for each recommendation and the benefit it provides. The more risk addressed, the greater benefit to the organization. Where appropriate, Vigilinx may recommend relaxation of existing security measures that cost more than they're worth.
3. Scorecard: The VBSA tool produces a "report card" for the organization. This enables executives to understand, at a glance, where they stand with respect to others in their industry. It also enables management to "re-test" the organization on a regular basis, to track repeatable processes and identify regression before it becomes a problem.

Driving Down Cost

The biggest benefit of VBSA is its unique ability to get executive information into the hands of those that need it for significantly less than any other effective assessment offered today. The basic, initial assessment starts at $30,000. Vigilinx offers a number of pricing options, including reassessment and quarterly programs. To find out more, contact a Vigilinx account representative or call us at 866.481.4101.

Conclusion

A useful security assessment has the following qualities:

- Standardization: Assessment criteria are tied to a comprehensive security standard.
- Industry Specificity: Industry best practices are considered to ensure that results are meaningful within the context that the criteria are applied.
- Ease of Understanding: The assessment findings and recommendations should reflect the environment in which they are made.
- Quantitative Measurement: Prioritization of the recommendations should reflect the objective measure of risk they eliminate.
- Non-trivial Observations: The team performing the assessment should have the know-how and experience to properly judge the importance of security findings and make workable recommendations.

Only Vigilinx combines these qualities through its proprietary VBSA tool and the broad experience of its security consultants.

Vigilinx Digital Security Solutions

Complete strategic security services, backed by the most advanced intelligence available anywhere. Vigilinx, the clear leader in digital security solutions.

Vigilinx Security Intelligence Service™

Vigilinx Business Security Assessment™

Managed Security Services
- Intrusion Detection
- Managed Firewall
- VPN

Technology Risk Assessment

Penetration Testing

Security Architecture Design

Integration Services

Information Security

Emergency Response & Forensic Services

Proactive Forensic Services

Corporate Headquarters

45 Waterview Boulevard
Parsippany, NJ 07054

866.481.4101
973.541.5400

www.Vigilinx.com
info@vigilinx.com

Regional Offices

New York, NY

Washington DC

Los Angeles, CA

Columbus, OH

Atlanta, GA

Minneapolis, MN

Dallas, TX

Vigilinx
Digital Security Solutions