INTERNET SECURITY AND DISPUTE RESOLUTION TECHNIQUES

C. Huber

ERNST & YOUNG
E-Security
Presentation to SAIMM
Introduction

To increase revenues, profitability and market share and to remain competitive, companies must be prepared to execute new business strategies quickly, efficiently and securely. To address increased risks and critical success factors, management needs to approach the control and security of mission critical assets on an enterprise-wide basis, allowing an organisation to develop and/or maintain its strategic, competitive advantage. Security policy and architecture should combine both proactive and reactive security services to mitigate risk and ensure that the proper policies, procedures and resources are utilised in the event of a security incident.

These are the following stages required:

- Determine current state as compared to best practices.
- Perform gap analysis.
- Create a project plan based on priorities and time frames.
- Establish security policy.
- Establish security architecture.
Current state, gap analysis and creating project plan for e-security

Research must be performed on the major revenue generating business models. How is the business connected to business partners, competitors, employees and remote locations? Each of these connections represents a potential security threat.

Based on the business models, understand where there may be opportunities to augment the business model using technology (effectiveness), build a new revenue-generating model (growth) or deliver a service or product cheaper (efficiency). All of these situations are openings for security solutions.

Look for areas where availability, speed and security of information will be major issues to customers.

Consider where the business may be involved in mergers, acquisitions, or spin-offs and determine security risks for each of those situations.

Could the business be the next "hacker" headline?

Determine the existing resources for security and areas of focus for the internal client staff.

Determine how to align business objectives, technology and risk to achieve business goals. The objective of e-business security is to enable business to execute business strategies through secure solutions.
The development of a successful E-Business Security Policy

The cornerstone of a good security policy is the establishment of a comprehensive set of "rules" by which information systems are defined, accessed, and protected. The British Standard (BS 7799: 1995) Code of Practice for Information Security Management can be used as the basis for building this security policy. During this phase of Security Architecture development, highly detailed and customized security policies and standards are developed that will serve as the foundation for the rest of the architecture components.

The development of security policies, standards, and procedures is predicated on the following security principles:

- To ensure the confidentiality, integrity, and availability of sensitive information;
- To provide for the protection of individual, proprietary, mission critical, or otherwise sensitive information;
- To ensure the ability to maintain processing during and following an emergency;
- To ensure the auditability of security relevant information; and
- To ensure management and employee accountability for computing resources including data and information entrusted to them in accomplishing organizational objectives.

Because security must map to real business valuations of assets, threats, vulnerabilities, and risk, it is vital to align the process to key management to clearly understand their specific concerns and to set the tone for subsequent security policy definition. Moreover, consideration must be given to industry, regulatory, contractual and vendor issues and these should be included into the policy and standards model.

Security policy definition includes gaining an understanding of business and information technology strategies, assessing requirements for information security and creating customized security Policies, Standards, Guidelines/Best Practices, and Procedures that serve as the cornerstone to developing Security Architecture. All Policies, Standards, Guidelines/Best Practices and Procedures are logically interrelated and must overlap and constantly reinforce each other. Policies and Standards should also be "platform independent" enabling the organization to seamlessly scale its systems governance activity to accommodate new systems and technologies. Platform-dependent requirements will exist on the Guideline and Procedure levels.
The overall policy definition, including Policies, Standards, Guidelines/Best Practices and Procedures, should include the following broad categories:

- Corporate Information Protection
- Security Management
- Information Asset Classification
- Risk Management
- Compliance
- Certification and Accreditation
- Physical (and Environmental) Security
- Personnel Security
- Security Awareness and Training
- Security Incident Response
- Security Monitoring
- Network Security
- Security of Audio/Visual Communications
- PC/Workstation Security
- Security of Information Systems Operations and Support
- Encryption and Information Confidentiality
- Logical Access Controls
- Identification and Authentication Controls
- System Integrity Controls
- System Audit Controls
- Security in the System Development Life Cycle
- Business Continuity Planning
- Media Security
- Third Party Services

The Policy Definition Phase will entail conducting a thorough review of the current environment to include current policy levels, Policies and Standards currently in-place, and policy documentation needed to satisfy customer, business, legal, government, and hardware/software requirements. Through the process of documentation reviews and interviews with management and staff a clear understanding of the culture will be achieved. Expect to find both written and unwritten Standards and Policies. Written versions will typically take the form of a Standards and Procedures Manual, while unwritten versions are those practices that are generally followed but are not formally documented.

The results of the Policy Definition are used primarily in support of the Technology and Risk Profile; they serve as the foundation for information classification and resource management efforts. Technical Security Architecture requires Policy and Standards output in order to prepare the engineering design effort. Policies and Standards developed serve as the basis for developing a variety of information security programs in developing the Organisation Structure. Finally, Policies and Standards support the development of Minimum Security Baseline (MSB) requirements.
The development of a successful E-Business Security Architecture

E-Business security architecture should provide a framework for the application of a consistent and unified approach by which an organization may develop and improve information security within its business operations. Security Architecture describes an organization's detailed plan for developing, operating, and maintaining its enterprise-wide security architecture.

The plan must be based on the organization's Business Strategy, which provides a phased, top-down approach that begins with developing statements of business strategy and security policy, and proceeds to the classification of information assets and the development of a risk management strategy. A technical security framework can then be designed, on which the organizational, technical, and deployment specifications can be based. Finally, a framework for ongoing management and monitoring of security will be created.

Security Architecture should provide a consistent and unified approach to developing, people, process, and technical controls to allow the organization to appropriately manage risk without increasing the burden of day-to-day operations and costs.
Security Architecture

Objectives

The following objectives must be addressed:

- The architecture must illustrate that the organization is providing "due care" and "due diligence" in protecting corporate assets;
- The architecture needs to leverage existing groups within the organization that provide IT risk and implementation services;
- The architecture must enable the organization's security function to proactively provide its services;
- The architecture must not add significant additional workload to customers of the organization security function;
- The architecture must culturally transition security decisions to business-based risk management decisions;
- The architecture must enable a "first to market" philosophy;
- The architecture must be simple to understand and as transparent to customers as possible; and
- The architecture must convey a standard and consistent message.

The Value of Security Architecture

An investment in building a structured Security Architecture will provide the following value to an organization:

- The architecture will reduce risk to business assets;
- The architecture will reduce costs associated with reactionary or crisis management activities;
- The architecture will proactively position the organization to deal with real-time incidents and emergencies that require immediate attention;
- The architecture will produce a solid structure to safeguard the organization's most critical assets;
- The architecture will allow the organization to more accurately plan and budget for the delivery of security both tactically and strategically;
- The architecture will provide a structured security vision to communicate the value of security throughout the organization;
- The architecture will permit education of organization security function customers on the value and importance of security so that they are aware that security is everyone’s responsibility; and Security Architecture Components
The Security Architecture should contain the following nine essential components:

- Business Strategy – sets the overall direction and scope of the organization's security function and allows it to deploy resources through the most cost-effective means possible;
- Policy Definition – documents the functional security business rules of the organization;
- Technology Profile – permits identification and classification of all critical assets of the organization;
- Risk Profile – provides for the identification and prioritisation of risks to organizational information assets;
- Technical Security Architecture – provides the technical framework for the architecture;
- Organizational Specifications – defines processes for managing the architecture;
- Technical Specifications – provides the native technical controls required to harden assets;
- Pre-Implementation Specifications – provides reports to facilitate effective implementation of the architecture; and
- Manage and Monitor Security Controls – establishes the means to operate and maintain the specific organizational and technical security controls.
Service Level Agreement
presentation to SAIMM
Three forces drive e-Procurement:

- **Speed**: The speed at which fulfilment takes place. Accelerated product life cycles. Real time responsiveness.
- **Connectivity**: Everything is becoming electronically connected to everything else (products, people, companies). There is a dramatic increase in the transmission of electronic data.
- **Intangibles**: Information and relationships are key in the e-procurement process. The service component of products is becoming key.

All 3 forces must be considered simultaneously.

The key to e-procurement is a well-defined and monitored service level agreement. The service level agreement and the monitoring thereof are vital in dispute resolution when it comes to e-procurement. The service level agreement will also cover areas around information sharing. Before an investment is made in the technology that supports e-procurement it is essential that service level agreements are established and supply processes are reviewed.

E-procurement is about the connectivity between the customer and supplier and the sharing of information that speeds up the process. Technology merely aids the transfer of information.
The development of a well-defined and monitored service level agreement

There have been a number of failures in e-procurement. Some have been high profile. These failures have been a result of poorly established service level agreements. The establishment and monitoring of the service level agreement is a key 'value add' that the portal or e-procurement system should offer.

Successful e-procurement is based mainly on the non-technology issues. There needs to be an open channel between the customer and the supplier. This channel involves the creation of a combined steering committee between customers and suppliers. There need to be regular meetings that focus on issues that arise as a result of the service level agreement.

In the past there have been antagonistic relationships between customers and suppliers. This antagonistic relationship is the main stumbling blocking in e-procurement. Information sharing and trust is key in e-procurement.

Companies have used EDI extensively in SA. The future of e-procurement is likely to be a hybrid between EDI and Internet technologies. The Internet provides the opportunity to share information more efficiently. The Internet linked with the development of new technologies also creates the opportunity for a multi-channel approach to e-procurement. Wireless technologies will be an essential part of e-procurement.

EDI is an initial phase of e-procurement. The next phase is actually sharing strategic information between both customer and supplier. The information that is communicated has very little to do with price, which currently is a misconception. For e-procurement to function at optimum, information sharing needs to relate to order fulfilment. This is where the service level agreement is vital in dispute resolution, as both parties have to agree to penalties and controls that are instituted. The customer will have to make commitments in terms of the timeous sharing of correct and complete information. The supplier will commit to order fulfilment. Fulfilment includes delivery points, package size and completeness of order.

In establishing a service level agreement the first phase is establishing a steering committee between the supplier and the customer. This steering committee will have the task of analysing the process changes required between the customer and supplier in meeting the requirements of the service level agreement. Furthermore, penalties relating to failure in terms of delivery or to failure in terms of supply of information or late payment need to be developed up front and monitored.
A blurring of boundaries takes place in that customers share their strategies with suppliers. Strategic information enables the supplier to supply the customer in the way they require.

For suppliers, customer relationship management is the main issue. Technology merely acts as an enabler of this relationship, providing faster, quicker and more accurate information. Suppliers really need to shift their relationship level up to a strategic one. Procurement has the ability of becoming strategic and of providing a competitive advantage.

E-procurement in its final form leads to inventory management by the supplier on the customer's premises. The service level agreement should be built with this in mind. This is a massive mind-shift. It depends on the information that is available between the customer and supplier. This is an extension of the blurring affect where the supplier becomes part of the customer's business and strategic team.
Conclusion

E-procurement is not about the available technology. The process developed to manage the relationship needs to be robust. E-procurement is about developing and extending relationships. These relationships lead to process changes and these processes are supported by technology. Dispute resolution is less of an issue in an environment where information is shared openly and effectively between customer and supplier. Dispute resolution between customer and supplier is really about establishing a strong relationship and continuously meeting to discuss issues around the service level agreement.