A Strategy for Information Security: TOGAF

L. Ertaul[1], A. Movasseghi[2], and S. Kumar[2]
[1]Math & Computer Science, CSU East Bay, Hayward, CA, USA
[2]Math & Computer Science, CSU East Bay, Hayward, CA, USA

Abstract - *In the old culture of security concept, information security was based on securing the ownership of information. This kind of protection accomplished through monitoring and securing the physical network devices and application software. In the new paradigm, which is entirely based o distributed network architecture and relationship within and across different enterprises that each uses a combination of non-proprietary and also proprietary information, the information and infrastructure access requires far beyond only the physical perimeter. In this new paradigm the technology team, policy makers and the legal advisors require a dynamic inter-action. Based on the current available TOGAF (The Open Group Architecture Frame Work) security information, this paper proposes a framework to provide information security at the enterprise-level which reflects recent realities of information and access sharing in enterprise networks...*

Keywords: Enterprise Security Planning, Information Security, TOGAF

1 Introduction

Today's globally distributed network systems require a management team that manages the viewpoints of all the stakeholders in the business, to collect objectives from each department and provide a solution that covers all their security requirements. [1]

The type of stakeholders that enterprise security architecture and also information technology team need to work as a single team include risk-management, corporate legal console, security auditors and different business managers.[1], [2]

This paper proposes a process-based, dynamic, information centric security framework which through different functional boundaries will help in resolving different viewpoints, and also provide a methodology for security policy both within and across the enterprise networks perimeter using TOGAF (The Open Group Architecture Frame Work) .

2 The Security Problem

One reason to analyze the current security effectiveness of information security policies is due to fundamental changes in the basic assumptions which those policies are based upon such as, by securing the physical perimeters of the information now the security of that property is achieved.

The history of securing the physical devices (hardware), applications (software) and the storage media is dating back to 1983 (Department of Defense Trusted Computer system Evaluation Criteria).[3] Enterprises for the past twenty years invested part of their budget for securing computing equipments, operating systems, communication channels, and storage properties. These properties are no longer requires security and in fact the computing platform is so much available to public that no longer is consider as a property.[1], [2]

What once were consider highly secure resources only thirty years ago such as storage, CPUs, network connections, and memory, are available today virtually anywhere, anytime. Yet the way business managers, decision makers, technical members, and others have learned and thought to handle the security of their data is by protecting their computing platforms and resources. [1], [2]

In today's globally distributed information networks constantly requires that all the sectors, private/public and other consumers to assume a new type of risks. At the same token, the people are responsible to manage these new types of risks seems not to understand and familiar with these issues adequately. [1],[2]

Industry groups, policy makers, interest groups, and regulators are working together on developing a new regulations and standards that can help the enterprises to control and manage the security of their information systems.

3 How Information Security Achieved?

The term "security" is usually used in two scenarios. The first can be thought as set of functions and features to protect integrity and confidentiality and also the availability. This case of security is well known and developed by the users and vendors alike, which resulted in broad selection of tools, application and standards that available for consumers. The TOGAF security group currently does not make a major contribution that differs from what other standards are already providing. [1],[2],[4],[5]

In second scenario, the security is thought as a property of the information systems such as usability, manageability and quality. In this term, the security is assumed as a non functional property which makes this property more difficult to measure and discuses clearly.[1],[2]

This paper explores this non functional part of security, to give some definition and also provide some strategy which can be used in conjunction with TOGAF security standard.

4 Enterprise Information Security Architecture

The architecture of enterprise information system consists of managing the viewpoints between consumer, business, and public sectors interests and provides a common resolution as shown in Figure 1. These interests include:

- Consumer expressed their interest to control the use their information's by both public and business sectors. This can be achieved by government help through regulations and legislation to prevent the misuse of those information
- Public, such as public safety, infrastructure protection from cyber attacks, national security, financial risk management and consumer protection.
- Business interests to provide environment to achieve the highest financial outcome for their shareholders and balance the risk and rewards. To provide higher return by minimizing the risk. The information security in business sector is viewed as risk management issue which can be resolved in favor of business goals.

The information security architecture objective is to mitigate the tensions between three sectors by developing non functional security components. [1][2][4][5]

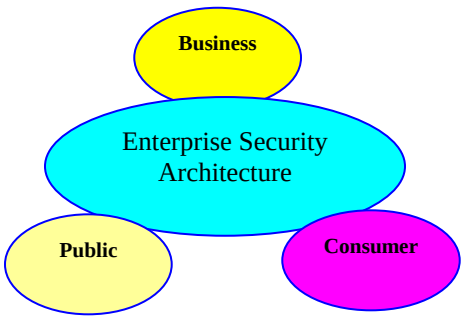

Figure 1 Enterprise Information Security Architecture

5 Closed perimeter vs. Centralize Information

In past the information security used to control the resources such as storage, computing and communication channels security by defining a closed perimeter by controlling:[1][2]

- Information access
- In/out traffic
- Time of access
- Entry port and type of service
- Resources to access computing platforms and speed
- Network connectivity access and bandwidth
- Storage media

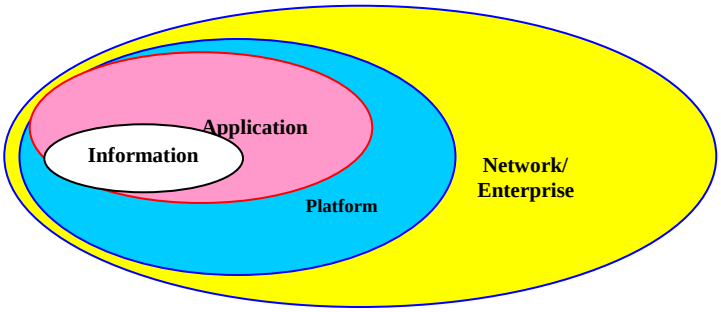

Figure 2 Layered Perimeter based Security Model

In today's networks, due to change of paradigm with vast availability of resources, the new paradigm requires support of supply chains, outsourcing, and other type of business needs. Current network perimeter security, Fig.2, concept have been shrinking and even in some cases disappearing that they not have a great control over major portion of communication and traffic passes through each boundary such as web, email, VOIP, and some type of encrypted data (SMTP, VPN). In new model, perimeter still exists, but changing to type of perimeters with no specific shape. The information can traverse between traditional boundaries with a shape that is not very clear to inexperienced security architecture.

Figure 3 Centralized Information Security Architecture

The question comes to mind that "How a security architect can establish a security quality for something as intangible as information by using non functional security model?"

At this point we have entered a new model and paradigm called "Centralized information" security as shown in Fig 3.

This new model which is shapeless with not clear perimeter shows that the traditional boundary such as platform,

application and enterprise perimeters does not exist any longer. Instead, this shapeless boundary surrounds the information from one entity to another.

6 Information Control

In our current model of shapeless boundaries, control of computing assets such as information which is intangible can be functionally equivalent to having "ownership" of physical assets in physical world. The new security definition becomes a question of being able to maintain an equivalency of "ownership" in traditional model through control over the computing assets such as information wherever in enterprise/network they reside. Based on that, following are the major principles of control that emerge:[1][2][4][5]

1) The assets can only be controlled within specific boundary, once the asset/information traverse outside the controlled environment, the control of the information by the owner has lost.

2) Remote control is hard; it's hard enough to control information within a managed application such as firewall perimeter. Controlling the information beyond enterprise boundaries is very hard to manage and guarantee. One way to resolve this issue to enable the global enterprise to share its sensitive information with suppliers, business partners, customers and outsource providers by an acceptable level of risk. This can be establish through:

- ❖ NDA
- ❖ Information sharing legal agreements
- ❖ Control expectations through standards
- ❖ Control practices for technical, physical entities that can be verified

7 Information Control within Virtual Boundary

TOGAF [4][5] presented a framework for security control for securing the information within enterprise virtual perimeter. This framework consists of:

- ➢ Define the requested action and how to response
- ➢ Monitor the incoming actions
- ➢ Force the action to be taken

as shown in Fig 4.

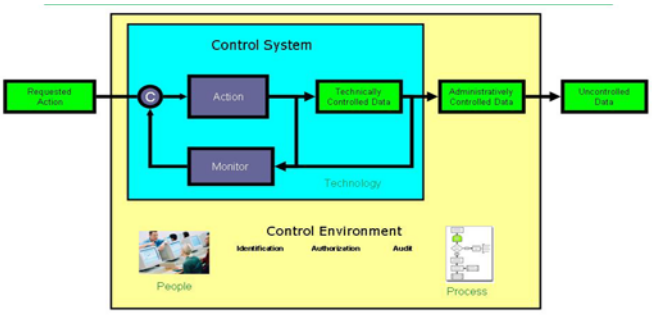

Figure 4 Virtual Frameworks for Security Control

8 Security Policy Compliance

To be able to control the information beyond the traditional boundaries, it's appropriate to discuss the role of compliance with security standards and policy such as TOGAF recommendations.

The security compliance model works in away that the enterprise security policy complies with standard and external policies such as TOGAF security architect framework as shown in Fig 5.

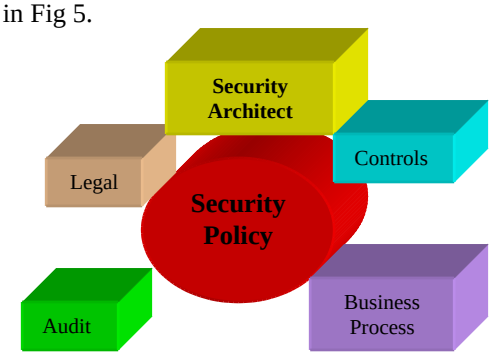

Figure 5 Security Policy Framework

Following are the major actions required for deploying a successful security police in enterprise environment:

- ➢ Define Compliance Goal – By answering "What standard security policy needs to be compliance?". TOGAF security framework can be used as the starting point plus other external requirements such as SLA (Service Level Agreements), customer expectations and corporate policies.
- ➢ Evaluate and Assess above Objectives – For the above objectives, the legal team must assess these requirements and check to see which can be apply to the enterprise and the business.
- ➢ Create Enterprise Policy – Not legal objectives in nature must be reviewed with business management and process people to create a policy that is consistent with the above objectives.
- ➢ External requirements compliance evaluation – Evaluate the security policy through legal team. This

team provides a document and the monitor that followed across enterprise organization.

- The Security Architect must implement a framework such as TOGAF that compliant to above security policy.
- Security Policy Audit Function – To assess whether the enterprise security process and technology comply with the enterprise generated security policy and also assurance that the management has been carried out these policies.

Information control beyond the enterprise control environment in general requires sort of formal agreements such as Service Level Agreement (SLA). To extend the control beyond the original perimeters, this control consists of:

- Generate formal agreement to control flow of information across involved enterprises perimeters
- Provide an SLA and a way to audit compliance

SLA is a legal and business management process. Audit and verification of compliance to that SLA can be achieved through standard audit framework known as SAS-70 (statement on Auditing Standards-70) report.[6]

SAS 70 audit is a highly specialized audit conducted in accordance with Statement on Auditing Standards (SAS) No. 70, Service Organizations. The product of a SAS 70 audit is presented by the auditor to the service organization in the form of a Service Auditors Report. The SAS 70 Service Auditors Report can be either a Type I or Type II. Advanced provides both types of services, as well as pre-SAS 70 assessments.

This report can help the enterprise to avoid conducting regular audit of critical systems; the enterprise information owner can request SAS-70 report from the vendor. From this report the enterprise security team can assess the degree of vendor compliance, which helps the enterprise security architect to evaluate if the vendor meets the information's owner expectations for control and manage its information.

9 Conclusions

Whether called "Centralized information security" , "virtual-boundary" or "control of information devices", the information security team must consider impacting factors such as policy, technology , and economic for information security. The team also required to represent all the stakeholders "views" within the process. Security as a combination effort of people, technology, and processes in enterprise architecture framework is controlling the information security across the organization perimeters. Based on these requirements, in today's information security strategies, corporate policy/legal, and the audit are the major stakeholders, which force the architecture community to articulate these stakeholders within the community.

The security architect can mitigate and facilitate the different view points of the stakeholders through providing a dialog between them.

TOGAF open group security division as a leading organization contributes toward providing solutions for security information. In this role the open group team facilities and encourage development of open standards, tool, and method to improve current enterprise security information essential practices and methodology. Some of the highly relevant components to support the security strategy are listed as:

- Even though auditing and monitoring are the key components of the security, but not many standards in these areas. What and what not you should monitor? This can be a joint project with legal team to clarify what should be monitor.
- Integrate with TOGAF monitoring and required corrective actions as a development of additional views on control.
- For compliance, develop additional views.
- Form a information security perspective with the help of legal, technical and audit members.

10 References

[1] B. G. Raggad, "Information Security Management: Concepts and Practice", CRC Press, 2010.

[2] H. H. Carr, C. A. Snyder, B. N. Bailey," The management of Network Security: Technology, Design, and Management Control", Prentice Hall, 2010.

[3] NIST Document DoD 85, "Department of Defense Trusted Computer system Evaluation Criteria" http://csrc.nist.gov/publications/history/dod85.pdf

[4] The Open Group web site: TOGAF
http://www.opengroup.org/togaf/

[5]: The Open Group Security Forum:
http://www.opengroup.org/security/

[6]: The Systems on Auditing Standards (SAS-70) report
http://sas70.com/sas70_overview.html