Role of Security-Charter in the success of your organization

Last Revised on November 2004.

Executive Summary (The Changing Business scenario):

Today more than ever, organizations are under pressure to deliver business solutions with maximum cost effectiveness while retaining appropriate service level. This attitude has changed the role of IT in the work place from a *business support function* to a *business enabler attitude*. With IT in business enabler space, it (IT) becomes a core component of business strategy. Whether one likes it or not Information Security and Assurance has a vital role to play in the balance of this whole equation of business economics.

This white paper looks into the trends that would help today's global businesses take a standard approach in Information Security through a matured structured methodology. This methodology would help in the realization of business strategy and achievement of business goals.

We have seen and heard about Information Security Policy and Standards and also Policy and Procedures. But rarely do we hear people talk of these three functions along with Guidelines and Forms. All of these have a finite role in the success of any organization and we are going to take a fresh view of all these from the viewpoint of Information Security and Assurance. Nobody will dispute the fact that organizations are always interested in better ways to manage and increase their overall productivity, but not many are working towards enhancing the poorly integrated and tactically incapable elements of the present Information Security environment. We need to change this. People, Processes and Technology are crucial to the success of Information Technology. We are going to talk about the middle factor – *Processes* in this white paper. Big changes come in the waves fueled by the combined energy of few influential individuals supplemented by the key factor of technical augmentation of the present age. These technical augmentations may prove to be vital for global businesses from the viewpoint of Information Security & Assurance. Let me start with a quote from *Gartner Research - December of 2002.*

> ***"By 2005, 75 percent of institutions that fail to organize, coordinate and focus their Security efforts will experience at least one major Security violation with significant disruptive impact (0.8 probability)."***

This and other similar researches have led to the maturity of the field of Information Security and Assurance. Across the globe, people manning this newly formed division within organizations know how to protect company's Information assets; they do understand in the real world Information Security is a service of multiple processes and not a single product. They also understand the importance of Prevention and Detection as well as React and Respond. If that is the case then these newly formed entities within global organizations are in good shape.

But this is not always true! Let me explain why; for few seconds step out of your IT shoes and erase your IT knowledge and be one among the crowd. Let us now look into the two words; "*Sign-up*" and "*Sign-in*". To the ordinary world they mean quite the same. Not to you when you are in your IT roles. They do have distinct meanings. Let me quote another example; Look into these three words in the custom packaging conversations; "*Pack&Mail*", "*PakMail*" and "*PackMail*". Depending upon which part of the world you are in, they all point to different business entities. But in casual conversations they sound much like the same. For example if you are in UK, they all might point to the same entity of www.packmail.co.uk. But here is US the first two are two different entities. So you see the confusion?

This is the foremost problem in the Information Security arena worldwide today. We need to have a common Information Security language/terminology. Everybody irrespective of their geographical location should interpret Information Security terminology in the same connotation. When we talk of Information Security Policies, internal Standards, Procedures and Guidelines most of us overlap the respective functional definitions of these terms. That is not good.

Adoption of a Security Charter could help put some clarity within the enterprise with regard to Information Security. Let's look into what a Security Charter in an organization could look like, and what it could offer for the success of that entity. Let us take an example of how a midsize company with adequate availability of human resources at hand can design intelligent internal processes that could leverage its competitive edge by adopting a Security Charter.

Security Charter:

Security Charter is a system of practices that are agreed upon by the organization in general for their prescribed Information Security practice. The phrase *Security Charter* is used when addressing Information Security at a higher level and represents the whole system of practices (some people call it best practices). A Security Charter should eventually disintegrate into multiple Security plans. A Security Plan caters to the needs of different business domains within the organizational framework. A Security Plan (at times also referred to as

Charters of the present age:

1. ANSI
2. **BS7799** security requirements established by the British Government. It is the parent security standard of the present day's **ISO 17799**. ISO 17799 could be purchased from http://www.standardsdirect.org/ for less then US $200.
3. COBIT (**Control Objectives for Information and Related Technology**) requirements established by the ***Information Systems Audit and Control Association*** (ISACA), an IT auditors and Information Security professional consortium, providing a framework for assessing security programs, developing performance baseline and measuring performance over a period of time.
4. CASPR (Commonly Accepted Security Practices and Regulations) main aim is to provide a set of best practices that can be universally applied to any organization regardless of industry, size or mission.
5. Common Criteria (CC), a.k.a. **ISO**/IEC International Standard **15408**, provides a charter and a framework for defining security requirements from both features and assurances side in the IT products and services. However, it is not intended to measure the effectiveness of an organization's overall security program.
6. GAO's FISCAM (Federal Information System Controls Audit Manual).
7. GASSP (Generally Accepted System Security Principles) of I^2SF (International Information Security Foundation).
8. **ISO 13335** Guidelines for the management of IT Security. It defines a variety of security controls and outlines the framework for risk management. However, like ISO 17799, it doesn't specify the means for implementing security measures.
   - ISO/IEC TR 13335-1:1996 Information technology - Part 1: Concepts and models for IT Security;
   - ISO/IEC TR 13335-2: Information technology - Guidelines for the management of IT Security (GMITS)
   - ISO/IEC TR 13335-2:1997 Information technology - Part 2: Managing and planning IT Security;
   - ISO/IEC TR 13335-3:1998 Information technology - Part 3: Techniques for the management of IT Security;
   - ISO/IEC TR 13335-4:2000 Information technology - Part 4: Selection of safeguards;
   - ISO/IEC TR 13335-5:2001 Information technology - Part 5: Management guidance on network security;
9. ITIL (**IT Infrastructure Library**) is a customizable framework that defines how Service Management is applied within an organization.
10. MOF (Microsoft Operations Framework) provides guidance that enables organizations to achieve mission-critical system reliability, availability, supportability, and manageability of Microsoft products and technologies. It is a sub-set of ITIL with few additions.
11. OCTAVE (www.cert.org/octave) (**Operationally Critical Threat, Asset and Vulnerability Evaluation**) was made available by Carnegie Mellon's CERT Coordination Center. It provides measures based on accepted best practices for evaluating security programs.
12. Principles and Practices for Security of IT-Systems from NIST (National Institute of Standards and Technology).
13. Site Security Handbook from IETF (Internet Engineering Task Force).
14. **SysTrust**™ requirements established by the AICPA (American Institute of Certified Public Accountants).
15. ISF (**Information Security Forum**) brings together the knowledge and experience of the world's leading organizations to meet the increasing demand for solutions to information security problems.
16. TickIT is about improving the quality of software and its application.

Information Security Framework) should go into individual details in multiple functional areas of Information Security, some of those at an abstract level could be:

1. Acceptable Resource Usage
2. Access Control
3. Business Continuity & Disaster Recovery
4. Critical-incident Response
5. Data Classification and Management
6. Internal Audit
7. Internal Standards
8. Perimeter Protection
9. Physical Access
10. Privacy Principles
11. Remote Access of IS resources
12. Risk Assessment and Mitigation (Risk Management)
13. Third-Party Resource Sharing
14. Wireless Communication

For a detailed listing of information security controls for low, moderate and high impact levels that is also referred to as baseline security controls, please refer to NIST Publication SP 800-53, Appendix I that is available from http://csrc.nist.gov/publications/drafts/draft-SP800-53.pdf

The easiest way to understand a Security Charter is to look into some of the leading and mature Charters of the present age. Refer to the sidebar above. These Charters were designed by different entities with different motivations and philosophies to achieve different objectives. All do address different needs of Information, but may not be adequate for Information Security arena with one exception of ISO 17799. ISO/IEC 17799 procedures and practices cover a wide range of issues by addressing a number of Control Requirements that need to be in place to achieve the best-of-breed IT Security. For more Information on ISO 17799 please refer to the presentation URL at http://www.iso17799software.com/presentation/

It is very important to understand that adoption of a specific Security Charter may not resolve all the Security issues in an organization. This is where general decomposition of security functional areas comes into play. It is equally important to know that a Security Charter by itself will create a *systematic system* in an organization. This system will increase the *Security Awareness* of the user community and will largely benefit everybody in the end. When a system is introduced, it is easier to manage from the management side and easier to adapt from the user side. This is exactly what a customized Security Charter could achieve.

One can also follow these Charters on an AS-IS basis but then the domain of these charters may shrink. Usually the real benefit comes when organizations create a hybrid model by taking good practices from each one of these Charters and create their own customized/proprietary Security Charter. This ensures that one gets a chance to drop the practices that are not suitable for one's own organizational culture. This customized model could work towards an organizations own advantage. This customized hybrid Security Charter could further be named so that it reflects the policies of the organization. The best part in this whole process is that each organization irrespective of its size and geographical location will get a chance to adapt to a system that will just work for them, rather then getting one cookie cutter model that fits all.

Definitions of Information Resources Attributes & Services (IRA&S):

- **Authentication:** Verifying the identity of an individual or other entity on the network or on the system before allowing that person access to your organization's data.
- **Authorization:** Ensuring that only those with successful authentication and appropriate permission have the right to access (read, write, modify, and so forth) your organization's data.
- **Availability:** Ensuring that critical Information, services, and equipment are up and working for continuous and uninterrupted use by the user community.
- **Confidentiality:** Preventing unauthorized disclosure of any part of your organization's data to any person(s) or entity within or outside your organization.
- **Integrity:** Preventing corruption, impairment, or unauthorized modification of your organization's data and providing service(s) to validate the Integrity of Information. From a mathematical point of view Integrity could also be defined as:

  Integrity = Accuracy (Reliability) + Completeness
- **Non-Repudiation:** Is a process of binding internal and external user communities with the actions performed on an organization's data. The action could be an electronic transaction that has an ability to add, change or delete a record in the database.

  Non-repudiation capability is necessary for an organization to bind a transaction to an entity, incase the initiator deny his/her involvement in the electronic transaction with a particular action. In layman's terms, it is equivalent to a paper-signature in the electronic world.

Security Plan:

Information Security Plan formulates how key-Information-Security-activities can be undertaken. In other words it should be the framework for achieving an organization's strategic business goals, objectives and maintenance of Information Resource Attributes &

Services (IRA&S) like *Authentication, Authorization, Availability, Confidentiality, Integrity and Non-repudiation*. For more information on IRA&S refer to the sidebar above.

A Security Plan is a subset of a Security Charter. It identifies the rules that will be followed to maintain the *MSR* (Referred to as Minimum Security Requirement) in an organization. The Plan will spell out specific details in all areas of Information Security Management. The detailed plan usually starts from Information Security Policies and then moves on into Policy Implementation Tools (PIT) like internal Standards, Procedures, Guidelines and Forms.

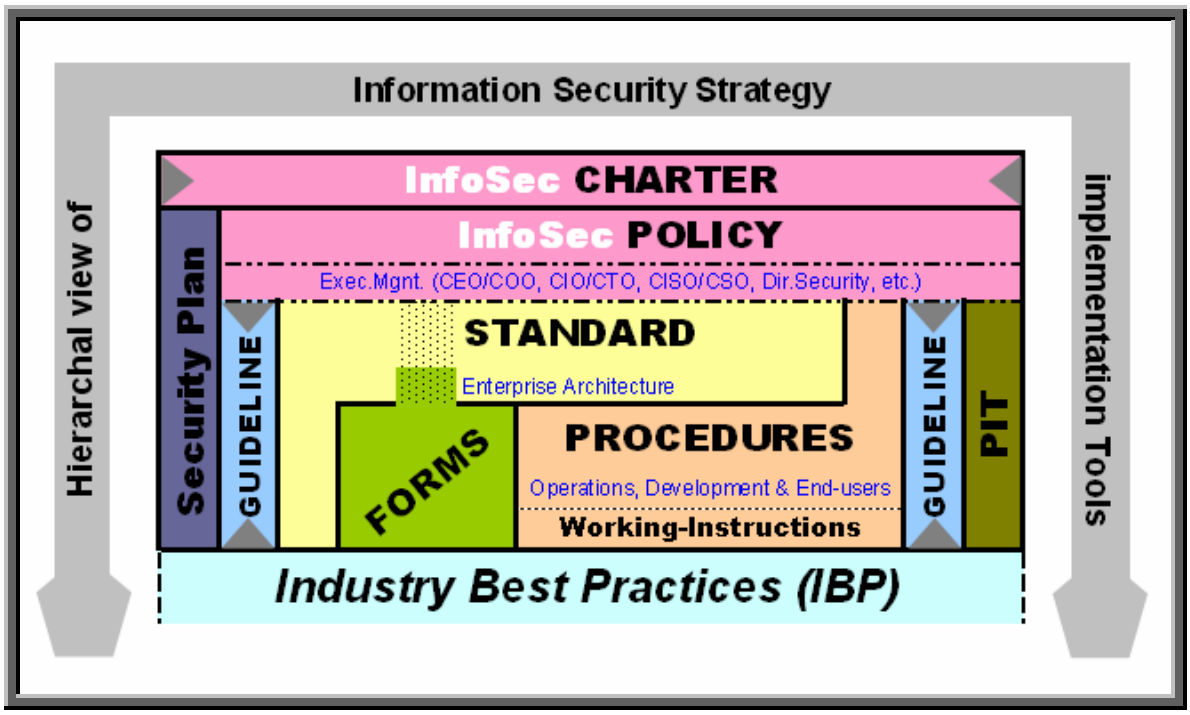

Figure 1: Hierarchal view of Organization's Security Policies and its relation with PIT.

Information Security Policies are made to support and achieve the core business objective/strategy. Human resource policies are developed based upon the issues whereas the Information Security Policy's are developed based upon the (Risk Model) risks posed by various factors in Information System's (IS) Functional areas at an abstract level. It is vital for these Information Security Policies to work; they should be endorsed by the executive management. Endorsement will get the required force and momentum into these Policies that can then become the driving force for the uniform enforcement of security policies in the entire stretch of the organization domain.

In order to uniformly enforce and propagate identified Information Security Policies, enterprises use different Policy Implementation Tools (PIT). PIT include internal Standards, Procedures, Guidelines, Forms or any other security control that can effectively be used to enforce a security policy. PIT has different coherent characteristics and distinct roles to play in the Information Security Policy enforcement process. Based upon the needs and the culture of an organization, a unique set of Information Security Policies and supporting PIT can be designed for unique organizational needs. This customized "Security Implementation Plan" could then become the Information Security Framework for the organization.

The *Information Security Framework* can then be merged with the enterprise document management system and be made to identify each document by a unique number, right from Security Policies to PIT. This sort of hierarchy would establish a one-to-one relationship between all organization's security policies and policy implementation tools (PIT). All these documents could be organized using numbering schemes similar to IEEE (E.g. 802.11b) or ISO (E.g. ISO 9001:2000) for document management and access purposes. This could then be served from a central location via the document management system with appropriate authorization to the entire enterprise.

If we look into the individual steps of the whole process of evolving a Security Charter and then coming up with a Security Plan and supporting PIT, then it could graphically be represented as in figure 2. Figure 1 represents the hierarchal view of different components of PIT and their relationship with each other.

Role of Awareness in Information Security:

A good number of information security breaches occur away from computer systems, terminal and access points. This includes, but is not limited too, careless placement of printed material, casual conversation and/or social engineering.

Security Controls do play an important role in the protection of Information Resources, but *Security Awareness* has an equally important role to play in the space of Information Security & Assurance. Talking of Security Awareness without Security Training would be a blunder. So let's look into both of these. *Training and Awareness* are twin functions in the IT space where one cannot stand without the other. Studies have shown that a company's biggest Security threat is its own employees. Based on this statement it could prove to be invaluable to organizations to take time to educate/train their employees about Information Security best practices and periodically test employees to make sure they understand *the Security basics*.

Training deals with the '*how'* aspect of education and prepares oneself to actually deal with a scenario/eventuality by developing specific needed skills, whereas awareness deals with the '*what'* aspect of education. It is also the so-called 'Social Marketing' that counters the negative effects of ignorance. A list of Information Security Awareness materials and activities is available from: http://csrc.nist.gov/ATE/awareness.html.

Figure 2: Formula that derives PIT. (Relationship between Security Charter, Plan and PIT)

Organizations are liable for the misuse of their technological infrastructure irrespective of who is doing it. Another most important undocumented function of Information Security and Assurance is

the coordination of Information Security & Assurance activities within the organization's different functional groups like Legal, Human Resource and Physical Security. The importance of this coordination is often over estimated. But the fact is the better the coordination, the better the overall security of that organization.

Conclusion:

We have seen that the world of Information Security and Assurance is full of challenges. Balancing the cost of implementing Security Practices versus the risk of not doing anything is the key to success here. To address these challenges there is a need for philosophical changes in the executive boardrooms for businesses to reduce their IT Risk exposure to an acceptable level. Disruptions are imminent but the potential payoffs are enormous for those people that align themselves with the right opportunity and with the right strategy.

A systematic approach of a *Security Charter* will certainly save time and money by developing organization-wide Information Security and Privacy Plans, a uniform methodology for implementing security enterprise-wide and much needed motivation and push for the workforce to move in the right direction. Best of all it would aid in the nourishment of a security culture that is badly missing in today's enterprise environment. A Security Charter will in turn provide a consistent approach and methodology for ongoing compliance of different industry specific regulations and for an organization's internal monitoring. A Security Charter could eventually become the launching pad for Process Certification and Accreditations like ISO-9001:2000, ITIL, ISO-17799, etc.

We should all work towards the goal of creating a global commitment towards Information Security and Assurance needs. We can do this better if we understand the underlying human factor beneath all these needs. We need to acknowledge that any System that ignores human nature WILL FAIL! Yet it is important to emphasize that Security at all times is always related to creating a cultural change. A cultural change is not achieved without a personal change. Remember that change is a part of *Revolution* and seldom a *Natural Phenomenon*!

About the writer:

Asad Syed, CISM, CISSP is a information security consultant. He is the CTO of Secure-bytes Com Inc. He has done Information Security Consulting at a global level for industries like Banking, Credit-Card, Fast-Food, and Pharmaceutical and now engaged with Healthcare industry in Chicago. He can best be reached by email at Asad@Secure-Bytes.com.

Disclaimer:

The views about Security Charter, Policy and PIT in this white paper are solely that of the author and may not represent the views of the company or companies with whom he is associated now or in the past or any of his professional affiliations. This white paper looks into the trends that would help today's global businesses take a standard approach in Information Security through a matured structured methodology. Author disclaims all warranties, expressed or implied, with respect to this white paper.

A closer look into Information Security Policy:

An Information Security Policy is a set of principles and objectives in a concise document mandating hi-level requirements, direction, rules and regulations that must be met by everyone touching Information resources of an organization.

An Information Security Policy should be made to support the organizations main strategy, goals and objectives. Security policies should embody a management's overall Security expectations, goals and objectives in a "non-technical manner" as a higher-level direction to its employees, its business associates and partners.

It is also good to have Information Security Policy to be point-specific and covering a single work area of a functional domain and not entering into the space of Security Controls because they by themselves will be a part of PIT. Information Security Policy should always be directed towards the safeguarding of an organization's Information Assets. It should be looked as a "mandatory directive" that could be uniformly enforceable with obligatory and disciplinary action when non-documented failure to comply occurs. There is a need for the management to have an exception handling process in place. A Security Policy should define corporate culture at a high level; for example what can and cannot be done.

An Information Security Policy should focus on Business Risk and should layout a system that is capable of minimizing the risk to an acceptable level. This is usually referred to as MSR standing for Minimum Security Requirement in InfoSec terminology.

An Information Security Policy should be implemented with the help of tools like internal Standards, Procedures, Guidelines and Forms. For a hierarchal and pictorial view of Information Strategy Implementation Tools please refer to figure-1.

Definition of an Information Security Policy:

There are multiple definitions that are documented and could be used. It is very important for organizations to have their own definition to create a common understanding across the workforce. If somebody asks me to define I would emphasize certain points like…

"An organization's Information Security Policy is part of the organization's Security Framework/Plan. A Security Framework is made up of multiple Security Policy documents. Each Policy document is a concise document that will help alleviate business risk by proposing achievable measures to take in order to mitigate the risks associated with the execution of business functions and addressing other non-compliance issues."

Security Policy should also establish the accountability of individuals in securing business resources by defining:

1. Exception process handling
2. Non-compliance issues and
3. By making organization's employees, associates and partners aware of various Policies and PIT (Refer to figure-1) that are in effect in an organization.

Issues related to Information Security Policy:

Few of the most visible issues in the deployment of Information Security Policy are:

1. Information Security Policy should be up-to-date in reflecting the organization's present strategy.
2. Information Security Policy should be effectively delivered and understood by the entire community. That in turn means that Security Awareness is a major part of an ongoing Information Security Policy lifecycle management.
3. There should be a process in place to track the compliance and measure the effectiveness of Information Security Policy propagation system. Without this it would be difficult for key Security people to justify the investment/ROI.
4. Information Security Policies should cover all major areas/domain of work, comprehensively. That means the length and breath of Information Resources of an organization should be addressed from all angles.
5. Information Security Policies needs to be in harmony with other organizational policies.
6. The most important part of the Information Security Policy Framework for an organization is to establish a MSR. While doing this it is important for management to realize that Security Policies could sometimes become a liability for an organization if they *have policies that are not enforced* and issues have gone to the court-of-law. This could be referred to as hitting with a hammer on one's own foot. So one needs to be very careful in designing and implementing an Information Security Policy Framework.

A closer look into internal Standards:

Internal Standards, Procedures & Forms are all set-of-tools that are used in the implementation of an Organization's InfoSec Policy. Internal Standards happen to be the 2nd step in the process of an Organization's Policy propagation. A Standard should always be a derivation from an Organization's Policy.

A Standard could be defined as a practice that is widely recognized or employed as a SOP (Standard Operating Procedure) in-house. It could be a benchmark or a degree of compliance or level-of-requirement that has to be met in the process of execution of a Procedure. The best example could be an organization's password standard that might say that all passwords in the organization should be a non-dictionary word of minimum 8 characters long with at least two digits in it and has to be changed every 4 weeks.

A closer look into Procedures:

Procedures are also the 2nd step in the organization's policy propagation process. Refer to figure-1 above. A Procedure should also be a derivative from an organization's Policy or Standard. Like Standards, Procedures when available should be mandatory to follow.

A good definition of a Procedure could be a configurational or procedural method or a set-of-instructions or a series-of-steps to perform a specific task that applies uniformly across the organization. A procedure could also be defined as an implementation-specific vivid step-by-step document explaining the execution of a task. When referring to exclusive details in a document to the level of a version, Procedures are sometimes referred to as "*Working Instructions*".

The best examples of a Procedure may be the sequential steps required in order to change a password of a Windows 2000 Server. That Procedure could talk about hitting Ctrl+Alt+Del and then clicking the Change Password button... and so on, or a document describing vivid details of hardening a base OS before placing the server in the company's production network.

A closer look into Guidelines:

A good definition of a Guideline could be a typical collection of configuration-specific or functional-specific or procedural-specific or system-specific *suggestions or aids*. Under this approach a Guideline becomes optional whereas Policy, Standards and Procedures are not. That means Guidelines are not requirements to be met, but on other hand are considered to be strong-recommendations to be applied at work when or where possible.

Guidelines could also be considered as the boundaries under which one can take a decision or perform a process. In this case guidelines become mandatory and the decision or process needs to be between the set limits. The best example of guidelines in this context could be the Federal Sentencing Guidelines that limit the judge's boundaries for sentencing. This specific interpretation of guideline does not apply in Information Security. ***In IS, guidelines are always optional.***

All – internal Standards, Procedures, Guidelines and Forms together are considered to be as the Information Security PIT. Refer to figure-1 for more info. They all provide specific interpretation of Information Security Policy to the audience in different scenarios.

A closer look at Best Practices:

It is a phrase that has been widely misrepresented. We should have a balanced approach in understanding and adopting it. A best practice for somebody is no practice for others. This is something that most of us fail to realize. Until we test a practice and prove that it works for us, it cannot generally be considered a best practice in that context.

Let's take an example of OS hardening procedure. There are many best practice documents out there; but if we pick one of them and apply it in our environment then probably our environment might stop working. *This is because something that works best for others, may not work the same way for us, as our environment may have some unique needs and requirements*. Hence, there needs to be a unique solution for every enterprise, based on the belief that enterprises do have unique needs and requirements.

Let us look into another best practice in password management space. "Keeping passwords a minimum of 8 characters long and a mixture of numeric, alpha-numeric and special characters will make it strong." Yes it certainly would! But what kind of best practice is this if one can get hold of a password-storage file from the OS and break it in 12 days instead of 2?

So remember, let us not make people happy by just giving them the narrow view. It is better to give a complete outline and help them develop a colorful version of it and let them decide what is best for them to practice rather than giving them best practices.

So to conclude a best practice is only best if it can help you increase efficiency & effectiveness of the processes in your environment.