Salesian Journal of Humanities & Social Sciences, Vol. V, No. 2 (December, 2014)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.05.2014.101-108 | Page No: 101-108 | Section: Article

Cyber Security Management

Dhirodatta Subba is an Assistant Professor and Coordinator, Department of Computer Science and Application, Salesian College, Siliguri Campus. He obtained his M. Sc (Mathematics) and M. Tech (Computer Science and Data Processing) from IIT Kharagpur. He worked with Tata Consultancy Services for 14 years before joining the College. He is associated with editing of the Salesian Journal of Humanities & Social Sciences.

Abstract

Our present world information systems consist of thousands of individual, interacting components. In the globalized network of computers the impact of local compromises extends beyond the boundaries of a single site. The consequences of penetration and the exploitation of vulnerabilities can be disastrous for the stakeholders involved. The complex nature of cyber space requires a multi-faceted approach involving a close partnership between Government, Industry and Academia for ensuring the security of information systems and assets of the country. Management of Cybersecurity calls for (a) implementation of policies into practice; (b) risk management that involves real time assessment, prevention and mitigation; (c) network monitoringand control - to detect intrusion, anomalies, vulnerability, infraction, security compliance, errors and carelessness in administration and operation of systems & network components; (d) ensuring that firewalls, routers, servers and workstations are equipped to repel attacks; (e) making software/hardware configurations secure by keeping them up-to-date in terms of patches & upgrades; (f) keeping malware protection in place; (g) user education and awareness; (h) facilitation in research. In this paper we will delve into the management aspect of the broad issue.

Keywords: Security Compliance, Industry, Education and Awareness, Management, Cyber Security

Introduction

Many different groups may pose a threat to a company's/organization's information assets: criminals interested in making money through fraud, operating not just as individuals but often in well-organized groups based in hard-to-reach jurisdictions; industrial competitors and foreign intelligence services interested in gaining competitive advantage for their own companies or countries; hackers who revel in the challenge of penetrating and disrupting computer systems and hacktivists who cause disruption for political or ideological reasons. And the insider threat should not be overlooked: potentially the actions of a company's own employees pose a risk, whether careless or malicious. Cybersecurity is a subject needing urgent attention in any organization today.

Salesian Journal of Humanities & Social Sciences, Vol. V, No. 2 (December, 2014)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.05.2014.101-108 | Page No: 101-108 | Section: Article

This article is based primarily on two sources: (a) *The National Cybersecurity Strategy Guide*[1] published by the International Telecommunications Union (ITU), Geneva. This document presents the *Ends-Ways-Means* strategy, primarily for national policy makers and (b) The white paper 'Cyber Prep' from MITRE.[2]

Further references to other standards/policies/guidelines are available in these two publications. Here, an attempt has been made to present a brief summary of essential points from both to give an overview of what it entails to put cybersecurity in place in an organization.

The ITU Guide

ITU has played an important role in global telecommunications, information security andstandards setting in different capacities since its formulation in 1865. ITU became theUnited Nations' specialized agency in the field of telecommunications, information andcommunication technologies ICTs in 1949. As the leading UN Agency on ICTs, ITU isthe global focal point for governments and the private sector in developing networks,services and mechanisms against threats and vulnerabilities.

ITU defines five pillars of the Global Cybersecurity Agenda (GCA), a framework for international multi-stakeholder cooperation on cybersecurity, as:

- Legal Measures;
- Technical and Procedural Measures;
- Organizational Structures;
- Capacity Building; and
- International Cooperation.

On top of the five Pillars, the GCA contains seven strategic goals:

- Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures;
- Elaboration of global strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime;

1 Frederick Wamala, The Itu National Cyber Security Strategy Guide, ITU, Geneva,September 2011. URL:http://www.itu.int/ITU-D/cyb/cybersecurity/ docs/ITUNationalCybersecurityStrategyGuide.pdf, accessed on 27.09.2013.

2 Deb Bodeau, Steve Boyle, JennFabius-Greene, Rich Graubart, Cyber Security Governance, MITRE Corporation, September 2010. URL:www.mitre.org/sites/ default/files/pdf/09_4656.pdf (accessed on 20/9/2013).

Salesian Journal of Humanities & Social Sciences, Vol. V, No. 2 (December, 2014)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.05.2014.101-108 | Page No: 101-108 | Section: Article

- Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for hardware and software applications and systems;

- Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives;

- Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials across geographical boundaries;

- Development of a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors and in all the above mentioned areas; and

- Proposals on a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

As applied to national context, the Figure A in the next section summarizes the key concepts.

Capability Maturity Model (CMM)

Software Engineering Institute (SEI)[3] has been in the forefront since 1991 in defining the maturity of an IT organization. The Capability Maturity Model has been accepted all over the world and is a de facto standard with respect to which any IT organization (or IT division) is assessed. The framework has been further enhanced incorporating the three source models: (a) Capability Maturity Model for Software (SW-CMM), (b) Electronic Industries Alliance Interim Standard (EIA/IS) and (c) Integrated Product Development Capability Maturity Model (IPD-CMM) - into a single improvement framework for use by organizations pursuing enterprise-wide process improvement. Fundamentally, the framework categorizes an organization into five levels: Initial, Managed, Defined, Quantitatively Managed and Optimizing.

The goal of an organization is to improve from one level to the next, towards excellence.The purpose of CMM Integration is to provide guidancefor improving an organization's processes and ability to managethe development, acquisition, and maintenance of products or services. It places proven approaches into a structure that helps an organization appraise its maturity or process areacapability, establish priorities for improvement, and implement theseimprovements. Aselected CMMI model can serve as a guide.

3 http://www.sei.cmu.edu/cmmi, accessed on 14.09.2013.

Salesian Journal of Humanities & Social Sciences, Vol. V, No. 2 (December, 2014)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.05.2014.101-108 | Page No: 101-108 | Section: Article

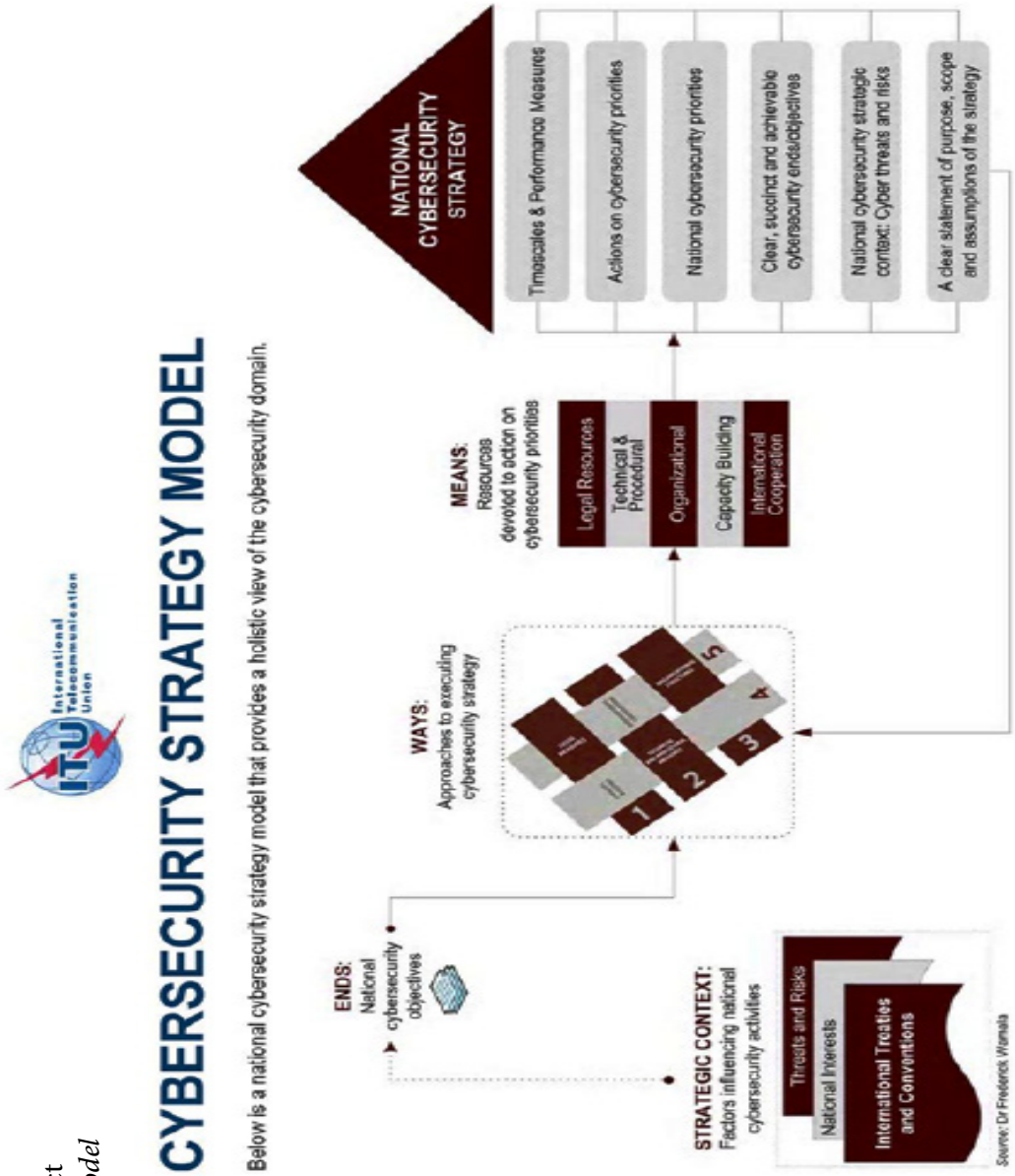

Figure A

The '
What' aspect
A. The ITU model

Level	Strategic Integration	Allied Disciplines	Risk Mitigation	Adaptibility& Agility	Senior Management Engagement	Risk Analytics
Pervasive Agility(5)	Full integration of cyber security into the organization's mission asswance strategy	Physical security, persorinel security, business continuity, SCRM, ICT architecture, business process engineering operations security, and cyber security are integrated with mission assurance.	Cyber security bufids on standards oS good practice, but pushes the state of the art to ensure continued security evolution in the face oS an innovative adversary.	The organization has defined, implemented and exercised a process that preventsor provides for alternate cyber decision making, allowing for timely decisions and delegation of responsibfiities, in the event that the adversary's actions results in a successful long term destruction or severe disruption of the primary decision making process.	CEO or Agency headactively engaged in mission assurancedecision s; senior official responsible Sor cyber secwity strategyclosely coordinates with near-term decision-mAers; some near-term decisions are reserved for the CEO or agency head(or designated senior official(s)in cases of disruption).	The organization models different adversaries separately. The organization continuallyupdat es threat models based on observations, indicators, assessed information from external sources, and closely-held information from trusted sowces. The response can be identified and managed dynamically. Thereis continuousassess mentof cyber risk factors.
Architectural Resilience (4)	Coordination of architectural and acquisition strategies with cyber secwity strategy.	Physical security, personnel secwity, business continuity, supply chain risk management (SCRM), ICT architecture, business process engineering, operations secwity, and cyber security are integrated with mission asswance.	Cyber security builds on standards of good practice, but pushes the state of the practice by incorporating state of the art techniques, sometimes at the expense of non- compliance with standards of good practice.	The organization has desined and implemented a process that provides for alternate critical cyber decision making a Mowing Sor delegation of responsibilities, in the event that the adversary's action results in a successsul long term disruption of key aspects of the primary decision making process.	Dedicated corporate officer or agency official actively engaged in enterprise-level cyber secwity decisions; closely coordinates with near-term decision-makers; some near-term decisions are reserved for the senior official (or designated alternate in cases of disruption).	The organization models different adversaries separately. The organization frequently updates threat models based on observations, indicators, and information from external sowces, so that the consequences of compromise and responsecan be identisied and managed. The organization desines and periodically assesses organization- relatedcyber risk factorsto inform enterprise risk management.

B. The 'Cyber Prep' model

The following is a summary of activities /components at each maturity level corresponding to the six key process areas.

Salesian Journal of Humanities & Social Sciences, Vol. V, No. 2 (December, 2014)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.05.2014.101-108 | Page No: 101-108 | Section: Article

Responsive Awareness (3)	Consistency between cyber security, architectural, and acquisition strategies.	Physical security, personnel security, business continuity, ICT architecture, and operations security are integratedwil cyber security.	Cyber security includes conformance with % standards of good practice, but pushes ie state of ie practice to address ie advanced threat.	The organization has defined a process that provides for limited alternate cyber decision making in i.e. event fat %e adversary's action disrupts critical aspects of the primary decision making process.	Responsible corporate officer or agency officialactively engaged in enterprise-level cybersecurity decisions.	The organization periodically updat es its threat model (or models) based on observations, indicators, and information from external sources, explicitly considering ie advanced persistent threat so fat i.e. consequences of compromisecan be identified and managed. The organization asseses common cyber risk factors using tool-based assessment as possible, and assesses ie organizational consequences of compromise of cyber resources.
Critical Information Protection (2)	Coordination of information security with business continuity.	Physical security, personnel security, and business continuity are aligned wit cyber secwity. Cyber security includes ICT, information, and communications security.	Information security is identified with % compliance wit standards of good practice, in i.e context of broader risk management.	The organization has an informal process intended to provide some limited alternate cyber decision making in ie event that ie adversary's action results in minor or short term disruption of some aspects of ie primary decision making process.	Information Security Officer or Information Security Program OViceractively engaged in information security decisions.	The organization periodically updates its threat model based on observations and information from external sources (e.g., CERT, ISAC, IiST industry members).The organization identifies business / mission dependencies oninformation resources, so that %e consequences of disclosure or comiption can be identified and managed.The organization assesses consequences of loss of information confidentiality, integrity, avafiability, and/or accountability.

Salesian Journal of Humanities & Social Sciences, Vol. V, No. 2 (December, 2014)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.05.2014.101-108 | Page No: 101-108 | Section: Article

Perimeter Defense (1)	No integration.	Physical security is aligned with cyber security. Cyber security is identified with ICT security.	Information security is identified with compliance with standards of good practice.	The organization's processes for decision making in the event that the adversary's action results in minor or short term disruption of some aspects of the primary decision making process are ad- hoc.	Program manager or business process owner actively engaged in information security decisions.	The organization updates its threat model infrequently, to reflect conventional wisdom (e.g., SANS, what is represented in relevant standards, what appears in the general business press, and/or what appears in the business press for the organization's business sector). The organizaẽon identifies high- value ICÑ resources (systems, applicaẽons, and communicaẽons). The organizaẽon assesses vulnerabùiẽes as produced by tools.

Table 1: Maturity mapping with key process areas

Salesian Journal of Humanities & Social Sciences, Vol. V, No. 2 (December, 2014)
ISSN: 0976-1861 | DOI: 10.51818/SJHSS.05.2014.101-108 | Page No: 101-108 | Section: Article

The METRE Guide

To address the Cybersecurity aspect, efforts have been made to define a framework similar to the SEI's.Cyber Prep framework enables organizations to articulate their strategies for addressing the advanced persistent threat (APT).

It defines five levels of organizational preparedness, characterized in terms of (a) The organization's perspective on, and/or assumptions about, the threat it faces (b) The organization's strategy for addressing the threat, including which adversary tactics, techniques, and procedures (TTPs) it addresses and (c) The organization's approach to cyber security governance.

The cyber security governance component of Cyber Prep focuses on what organizations must do differently from or in addition to generally accepted information security governance practices in order to address the APT.

Policy guidelines/frameworks generally describe what needs to be done. The next section presents the 'what' aspect

The 'How' aspect

Once the management is aware of the 'what' aspect, the next question is 'how' they should be done. Cybersecurity being a subject primarily in the domain of Information & Technology, most of the details are technical. However, there are other dimensions like the legal, international relations, human rights etc. Some of the pointers are listed below. They have cross references to other materials which cover the non-technical issues also.

- Federal Communications Commission (FCC, USA), Small Biz Cyber Planner, November, 2011.(URL: www.fcc.gov/cyber/cyberplanner.pdf)
- Seymour Bosworth, M. E. Kabay, Eric Whyne (eds), Computer Security Handbook, 5th Edition, John Wiley & Sons, Inc., 2009. This is a valuable general purpose guide for IT security.
- Industry experts like IBM, HP, Cisco, Raytheon, Lockheed Martin, AT&T, Honeywell, General Dynamics, Kaspersky …. to list a few - all of them have Cybersecurity solutions.
- Some IT consultancy & Services firms also provide solutions.

Conclusion

We have been through the top-down overview of cybersecurity management: the essential aspects of what it involves and how an organization can assess itself in terms of capability maturity. The 'how to' aspect being fully technical has not been elaborated much; only some references have been mentioned. Expert assistance is to be sought from professionals if an organization is serious about implementing it.