8-2004

Rating information security maturity

Arcot Desai Narasimhalu
Singapore Management University, desai@smu.edu.sg

Nagarajan DAYASINDHU
Infosys Technologies

A thought communiqué from Infosys

Cutting Edge

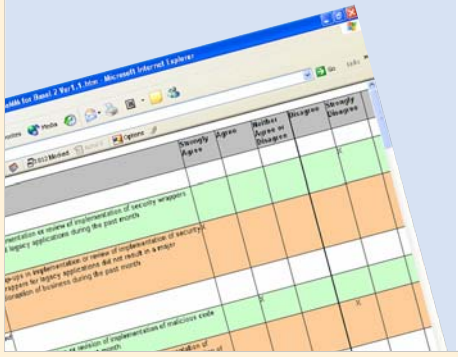
Rating Information Security Maturity

ARCOT DESAI NARASIMHALU & N DAYASINDHU

AUGUST 2004

Better be despised for too anxious apprehensions, than ruined by too confident security.

- Edmund Burke, Irish philosopher and orator



Executive Summary

In an address late 2001 at the Cyber-Security Summit, Richard A. Clarke, the then chairman of the US President's Critical Infrastructure Protection Board and special advisor to the President for cyberspace security, observed that the average company spent 0.0025 percent of its revenue on IT security - a little bit less than what most companies spent on coffee. He told them if they thought IT security was about the same priority for their companies as coffee they should not complain when they get hacked, and that they will get hacked. Mark Gerencser and DeAnne Aguirre from Booze Allen Hamilton, reported key findings from a survey of the CEOs of Fortune 1000 firms undertaken by RoperASW in the last two months of 2001[1]. Ninety percent of CEOs surveyed had reviewed their firm's disaster-planning documents since September 11 2001, and more than three-fourths had reviewed insurance policies to ensure adequate coverage and preparedness. These findings send home some important messages. Investment in information security certainly deserves a better treatment. However, most CEOs have difficulty relating to the level of information security investments considered to be adequate for their company. Secondly, several CEOs were keen that not just they but their business partners should also be safe from sabotage. *Is there a means for senior executive teams to measure the state of readiness of their companies for handling information security attacks?*

Measuring and Managing Information Security

Several information security frameworks and methodologies have evolved over the years. Apart from the likes of ISO / IEC 13335. NIST handbook, ISO 21827, SSE-CMM, OCTAVE, ISO17799 / BS7799, CDSA, CISSP and Common Criteria, there are also domain dependent audits such as OCC and SAS 70. These assist the information security teams to identify vulnerabilities and secure the information assets of their companies. However, they do not prescribe any means of informing the top executive teams about the state of readiness of their companies for handling information security attacks, both from within and outside.

The executive team of a major company cannot be expected to have the time and patience to go through the detailed findings of information security audits. They would be greatly assisted by a rating of their company's cyber security health and the recommended rating for an average company in their vertical. This would help them understand whether they are up to the norm or need to invest more. Those companies which like to position themselves at a level higher than the recommended rating can do so based on their core values and corporate governance principles. This would be akin to how companies approach environmental issues. A number of them try to abide by the minimum requirements whereas others would like to invest more as a means of differentiating themselves. Such a rating would also allow suppliers and vendors to assure their large corporate buyers that they have taken the requisite steps to be safe from sabotage.

Rating Information Security Maturity

Researchers at Infosys, in collaboration with Singapore Management University undertook a study on the maturity levels of Information Security to reflect the state of information security health of a company, including their level of preparedness to handle external and internal incidents.

The team developed an Information Security Maturity Model (INFOSeMM), a four level model which categorizes an organization into inactive, reactive, streamlined and proactive with respect to its current status based on a study of the IT security gap analysis. Each organization is assigned a three letter IT security maturity index. The ratings help the corporate manager responsible for the information security health of an enterprise to assess and report the company's IT security maturity level to its top management. This person could then use the index to engage top management on the benefits and pain points at the current maturity level and the desired rating. This helps the head of security to plan for IT investments commensurate with the desired positioning of the company as directed by

Maturity Level	Infrastructure	Intelligence	Practices	Index range
One: Inactive	Infrastructure (network, system and environment) is not secured.	Intelligence (application and data) is not secured.	Practices (people, process and management) are not secured.	DDD
Two: Reactive	Infrastructure is secured in response to incidents.	Intelligence is secured in response to incidents.	Practices are secured in response to incidents.	cDD, DcD, DDc to CCC
Three: Streamlined	Infrastructure is secured for known vulnerabilities through regular reviews and resulting revisions. The solutions are streamlined with other two pillars.	Intelligence is secured for known vulnerabilities through regular reviews and resulting revisions. The solutions are streamlined with other two pillars.	Practices are secured for known vulnerabilities through regular reviews and resulting revisions. The solutions are streamlined with other two pillars.	bCC, CbC, CCb to BBB
Four: Proactive	Infrastructure is secured for known and anticipated vulnerabilities through regular reviews and resulting revisions.	Intelligence is secured for known and anticipated vulnerabilities through regular reviews and resulting revisions.	Practices are secured for known and anticipated vulnerabilities through regular reviews and resulting revisions.	aBB, BaB, BBa to AAA

Table 1: Maturity Levels, Rating Index, and Enterprise Characteristics

Source: Infosys Research

its top management. INFOSeMM also helps enterprises to attain a level of IT security maturity that leads to customer confidence, regulatory compliance, reduction in insurance and legal costs, and frees the top management time for focusing on strategic business issues.

Levels of Information Security Maturity

Inactive Enterprises: These are enterprises that may be either ignorant of the impact of information security on them or even when were fully aware may not have the resources to respond.

Reactive Enterprises: These are enterprises that may have recognized the need to respond to such threats and may have been quite satisfied by committing initial investments. Such organizations are generally classified as Reactive Enterprises.

Streamlined Enterprises: Some diligent enterprises may have realized the need to address the continuing onslaught of cyber attacks and hence would have instituted regular review and revision of their level of preparedness. They would also have tuned the different security solutions to get a smooth end to end assurance.

Proactive Enterprises: Visionary organizations might decide to be proactive in their approach to managing such cyber attacks. These enterprises will be proactive in anticipating future attacks, drawing up suitable response plans and might even conduct simulated attacks to assess the level of preparedness of their systems and people. These enterprises will be operating in Level 4.

Not all enterprises need to operate at Level 4. The level at which an enterprise needs to operate will largely be determined by the industry segment in which it operates. Even where the industry segment requires an enterprise to operate at the highest level, there may be several applications within an enterprise which need not operate at the highest levels. For example, if we broadly divide the enterprise applications into internal and external (corporate and client facing), the internal applications can often operate at a lower maturity level than the external applications.

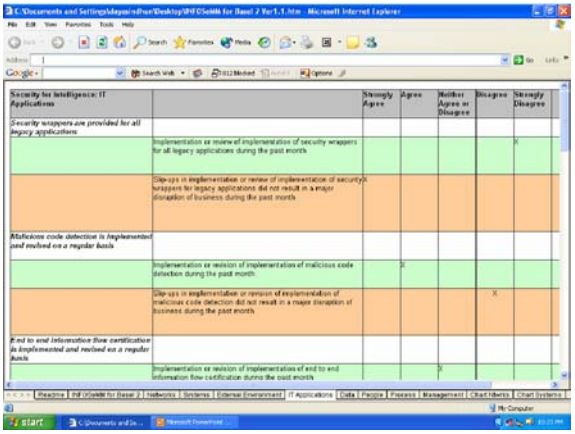
Managing Information Security Maturity by Infrastructure, Intelligence and Practices

INFOSeMM helps analyze eight sets of information security vulnerabilities in three pillars namely Infrastructure, Intelligence and Practices (Refer Table 1). Infrastructure consists of network, systems and environment, Intelligence consists of Applications and Data and Practices consists of People, Processes and Management. Each pillar can be assessed for its maturity level.

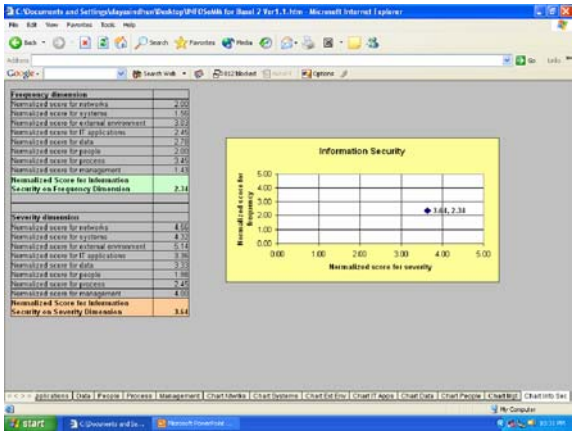
To effectively manage Information Security, enterprises will first need to assess their current maturity level. Once the desired maturity level is identified, transition plans to migrate to the desired maturity level need to be drawn up and implemented. Some enterprises may

Figure 1: Assessment tool and Executive Dashboard prototypes based on INFOSeMM

Source: Infosys Research



Assessment Tool



Executive Dashboard

prefer to make the transition in small steps in order to optimize the use of their resources. Others might be willing to migrate to the desired level in one step. This is a decision to be made by the executive management team of the enterprise.

Infosys consultants help enterprises to formulate transition plans using INFOSeMM keeping in mind the business imperatives. Transition plans for the vulnerabilities will assess the current maturity level and the recommended set of actions to be taken to get to the desired maturity level. The approach also helps enterprises to develop IT applications and systems mandated in the transition plans to enhance an enterprise's Information Security Maturity.

INFOSeMM is a useful approach that fits well with the current market realities that are compliance driven. A recent META Group research note observed that, "Although compliance mandates affecting G2000 organizations create new business opportunities for business and IT service providers, they also create additional challenges, overhead, and risks that providers must assess, understand, and manage.[2]" In this context, INFOSeMM can be used as an assessment method for Information Security, a Key Risk Indicator in Operational Risk category of Basel 2 compliance regulation. As depicted in Figure 1, the model can effectively be used to guide continuous assessments of information security in lines of business in enterprises, apart from providing a platform for designing executive dashboards for senior management.

Key Words: Information Security, Infrastructure, Intelligence, Practices, Maturity rating.

References:

1. Booz Allen Hamilton, How Corporate Security is Reshaping the Post 9/11 CEO Agenda, January 2002.
2. Stan Lepak, Responding to Compliance's Impact on Business and IT Services, META Delta, META Group, 19 August 2004

About the Authors

Prof Desai *is the Practice Associate Professor at the School of Information Systems in Singapore Management University. He was the scholar in residence at SETLabs during June-July 2004. Prior to joining Singapore Management University, Desai has spent more than two decades in leading computer science R&D labs. Desai has been involved in setting up CyLab ASEAN that will focus on cybersecurity an IT applications in association with Carnegie Mellon University. His current research interests information security management and innovation management. He can be contacted at desai@smu.edu.sg.*

N Dayasindhu *is a Senior Research Associate at the Software Engineering Technology Labs, Infosys. His research interests include IT strategy and IT outsourcing. He has published in peer reviewed journals and conferences as well as in the popular press. He can be contacted at dayasindhun@infosys.com.*

CE-08-04

Infosys®
POWERED BY INTELLECT
DRIVEN BY VALUES

Cuttng Edge is a monthly thought leadership note published by Software Engineering and Technology Labs (SETLabs) of Infosys.

Editor: Joseph Shields, Senior Research Associate (joseph_shields@infosys.com)