International Journal of Electronics Communication and Computer Engineering
Volume 2, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Information Security Strategy- A new approach

First Mrs. Aparna Chaudhuri, Second Prof. B.B. Meshram

Abstract **- Small and medium enterprises(SMEs) are gradually believing that information is an asset and like any other asset it needs to be strategically managed and protected. In most of the SMEs developing a strategy and then implementing the security measures are avoided or are considered as redundant. So in most of the cases it leaves loop holes in Information Security which result into threats and financial loss in the future. To improve security in a SME Purser's proactive approach, with a little modification, is especially helpful. In this approach the process of preparing the strategy is explained in eight steps.**

Index Terms**— Information Security strategy, Information Security strategy Plan, Security strategy for SMEs.**

.

I. Introduction

Information is an asset and like any other asset it needs to be strategically managed and protected. It is therefore imperative that leaders of organizations and particularly SMEs understand the value of information contained within their business systems and have a framework for assessing and implementing information security [2]. The information security strategy is a guideline for the future. This guides the SME to improve continuously and ensures that the organization remains focused on the important issues. The information security strategy should continuously change and accommodate the changing threat environment. So the strategic planning cycle generally consists of four phases[1] -

1. Definition of strategy
2. Production of strategic plan
3. Execution of the plan
4. Monitoring for further improvement

F. A Author Mrs. Aparna Chaudhuri is a Lecturer, Centre Point College, Nagpur, India. (Email: aparna.chaudhuri9@gmail.com)
S. B Author Prof. B.B. Meshram is the Head, Computer Tech, VJTI, Mumbai, (Email: bbmeshram@vjti.org)

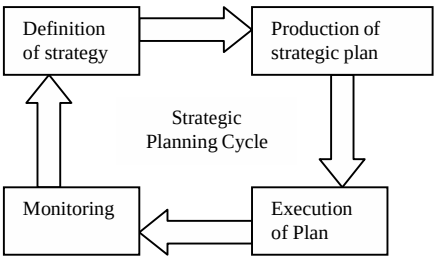

Fig. 1: The Strategic planning cycle

Appropriate information security strategy helps to improve organization security [4, 5]. Most of the organization ignore the strategy [6] and apply countermeasures at tactical level [7], which fails to utilize the measures optimally.
Information security strategy cannot be formed overnight. Initially ideas will be incomplete. Most of the SMEs will not be able to identify the final goal but the can surely understand the areas where improvement is required, this act as the intermediate goal.
The document is organized in the following pattern. In the first section we have discussed about different Types of Security Strategies,

II. Different Types of Security Strategies

According to Earl (2002), the evolution of SMEs in security terms is dependent on Information and Communication Technology (ICT) usage. It is important that IT security strategies in SMEs are reflective of the ICT usage. For instance, in
SME where there is limited or no ICT usage then there is no need to have an IT security strategy. For SMEs with sophisticated ICT usage, there is need to have a policy which addresses all issues about usage of their ICT infrastructure.[2]
There are different classifications of Information security strategy. They are –

1. Deterrence and prevention or Prevention
2. Limitation and correction
3. Isolate , exclude, isolate, exclude, restrict, recover and punish,
4. proactive and reactive,
5. Preventive and Reactive or Deterrence,
6. Detection, Delay and Response.

According to Sanseo Park and Tobias Ruighaver [3] there are three dimensions in information strategies. They are Time, Space and Decision making.

Time dimension - In time dimension strategies are employed based on the time of attacks. Different categories of attacks are used at different times. Proactive strategies are used before attacks while whereas Reactive ones can be utilized once the attack has recognized.

Space Dimension – In space dimension strategies are divided into bordered and layered. The defense mechanism in perimeter defense is placed at the line between internal and external area. Eg: Firewall at the network gate.

III. Decision Making Process Dimension

Decision making process dimension is used in military and business field.
Decision making process dimension is classified into three classes: Cognitive, Determinative and Directive.

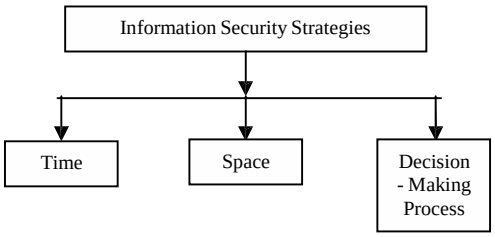

Fig 2: Classification of Information Security

IV. Developing the Information Security Strategy

The Information Security Strategy for a SME is developed in different stages.

Step 1: Analysis of the current situation
Step 2: Identification of business strategy requirements Step 3: Identification of legal and regulatory requirements Step 4: Identification of requirements due to external trends Step 5: Definition of the target situation
Step 6: Definition and prioritization of strategic initiatives
Step 7: Distribution of the draft strategy
Step 8: Agreement and publication of final strategy

In the first two steps the current situation is analyzed and strategic requirements are identified. For identifying the strategic requirement the major issues are considered and the requirements are derived from these issues. In third step these requirements are consolidated and verified for coherency. Then this complete list is then used to define the strategic goals. In the next step the strategic initiatives are prioritized. The high priority initiatives are considered to prepare the draft strategy which is distributed amongst all stakeholders. The draft strategy is modified and approved according to the suggestions of the stakeholders and the final strategy is prepared and published.

Step 1: Analysis of the current situation

In the first phase the current system if present is analyzed. This step takes the longest time to complete because most of the time the documentation of the current or previous system is not produced or is lost. The available documentations are poor in quality or outdated. Many of the staff members who were involved in preparing or maintaining the strategy have left the organization. This analysis confirms the known major issues as well as reveals a number of minor details which were ignored before.

Step 2: Identification of business strategy requirements

The business strategy of the SME ultimately decides the future IT requirements. So to develop an IT security strategy studying the business strategy helps to prepare a long lasting IT security strategy. But a properly documented business strategy is very difficult to find. If a documented business strategy exists only a part of it is accessible for review for security reasons.

Step 3: Identification of legal and regulatory requirements

The legal requirements usually decide what the SME can do with its systems and data. Some of the law which the data and systems are secured are – data protection law, privacy law etc.
The SME is concerned with the important legal requirements are in the areas of privacy and data protection. The SME needs to be compatible to other SMEs in the country and so the security mechanism must be compatible with the criteria published by the regulatory bodies.

Step 4: Identification of requirements due to external trends

The strategic requirements can also be influenced by external factors like changes in threat environment, changes in the economy, political events, mergers or change in technology etc. The IT strategy of the SME should be able to accommodate the risks like Spam, Malicious code etc.

Step 5: Definition of the target situation

The target situations are defined in terms of strategic requirements.
If there is a significant gap between the current security framework and threats associated with the modern technological development then strategic requirement is to design and implement IT security architecture capable of combating those threats.
If there is less communication between security department and the users then the strategic requirement is to ensure that all the users are well informed about the security related matters.

Step 6: Definition and prioritization of strategic initiatives

Before designing the final strategy a draft strategy is developed. The strategy requirements are prioritized according to a set of predefined criteria, typically reflecting the degree to which they mitigate risk, degree of difficulty and

cost. The high priority ones are taken into consideration. The draft strategy explains the major objectives that the strategy is designed to achieve and the background information that the readers need to know to understand the strategy.

Step 7: Distribution of the draft strategy

The draft strategy is documented in a proper manner and then distributed amongst all the stakeholders. The draft strategy contains all the objectives in detail and description of how they will be achieved.

Step 8: Agreement and publication of final strategy

The draft strategy is distributed amongst all the uses for approval. The users are requested to give their feed backs within a stipulated time. The necessary modifications are done and the final strategy is prepared and submitted to the authority. This strategy can now be implemented in the SME.

V. DISCUSSION

In previous researches it has been found that the SMEs have less access to adequate business and market information. They also lack reliable web presence and mechanism for online selling. They need to improve the knowledge and techniques to promote quality production and market presentation strategies. The need more information about the sources of financial assistance available in the market.
SMEs don't have expert IT staff and that is why they can't use the ICTs as effectively as larger companies. In future the SMEs are going to face increasing demands on IT capability. To remain in the market the SMEs need to remain competitive price wise and service level wise. To remain in the competition they need to use IT prudently so that they can handle larger orders and grab new export opportunities.
Since the SMEs don't have the expertise in handling the IT related issues they prefer outsourcing the job. But there always remains a gap between the organization and the web developers or contractors. The SMEs become dependent on these outsiders for the security of their own organization. The success of their business largely depends on the relationship and expertise of the outside partner. To get rid of the dependency the SME should increase awareness amongst the employees of the organization. For the same the SMEs should regularly hold seminars and workshops to educate their staff about IT security. To educate the staff the SME should have a very systematic approach. The best way to incorporate is to incorporate the training in the IT security strategy. So the modified steps are –

Step 1: Analysis of the current situation
Step 2: Identification of business strategy requirements Step 3: Identification of legal and regulatory requirements Step 4: Identification of requirements due to external trends **Step 5: Identification of requirement of training amongst the employees**
Step 6: Definition of the target situation
Step 7: Definition and prioritization of strategic initiatives
Step 8: Distribution of the draft strategy
Step 9: Agreement and publication of final strategy

Here we suggest a new step –

Step 5: Identification of requirement of training amongst the employees

In this step the training requirement amongst the employees to handle the IT setup of the company should be considered. The training should consider the technical and legal aspects. The training requirement should be specific to every employee depending on their jobs. The IT administrators and the users should get training according to requirements. If required employees can even be sent for certification programs so that later the Information security can be maintained by the SME.

VI. CONCLUSION

This paper explains a structured, rational approach that helps to develop an IT security strategy for a SME. It is important to plan the strategy very carefully.
The suggested change in the steps to incorporate the training program of the employees will help the SME to get the approval of the management and thus implementation will be easy. Since the training will be employee specific and job specific the allocation of responsibility will be done and after that the training programmes will be decided. Thus there will be better maintenance of security and better disaster management.

REFERENCES

[1] A practical guide to managing information by Steve Purser
[2] Adoption of information technology security policies: case study of kenyan small and medium enterprises (smes)
1Michael Kimwele, 2Waweru Mwangi, 3Stephen Kimani, Journal of theoretical and applied information technology
[3] Strategic approach to information security in organizations
Sangseo park and tobias ruighaver
Department of information systems
The university of melbourne

Parks@pgrad.unimelb.edu.au, ruighaver@optushome.com 2008 international conference on information science and security
[4] It security strategies for SMEs
Ji-yeu Park1, Rosslin John Robles1, Chang-Hwa Hong1, Sang-soo Yeo2, Tai-Hoon Kim1
International journal of software engineering and its applications
Vol. 2, no. 3, july, 2008
[5] E-business, SMEs and risks: towards a research agenda
Dr. Arun sukumar ,Department of management
Glasgow caledonain university, United Kingdom
A.sukunar@gcal.ac.uk, Prof. David edgar
Division of management, Glasgow caledonain university, United Kingdom , d.a.edgar@gcal.ac.uk , International journal of management innovation systems Issn 1943-1384
2009, vol. 1, no. 2: e4

[6] Information Technology (IT) security
Management in Kenyan Small and Medium
Enterprises (SMEs)
International journal of computer science and information technologies, vol. 2 (1) , 2011, 517-525 517
[7] eBusiness strategy optimizing usage of ICTs by Irish SMEs and microenterprises, Depertment of Enterprise, Trade and Employment, Dec,2004

[8] Strategic Approach to Information Security in Organizations by Sangseo Park and Tobias Ruighaver Department of Information Systems The University of Melbourne parks@pgrad.unimelb.edu.au, ruighaver@optushome.com.au
[9] "The Customer and Investor Access to Information Act of 1999" September 2003, http://thomas.locgov/cgi-bin/query/D?c106
[10] "Welcome to the Sale Harbour," August 2003, http://www.export.gov/safeharbor/index.html

