A Methodology for Measuring Information Security Maturity in Norwegian and Indian MSME's with special focus on people factor

Murali Krishna, Penmetsa

Master's Thesis Project Description
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2010

Avdeling for
Informatikkogmedieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

Information Security with focus on people factor has become a major focus area for all sizes of organizations globally. Because people are those in these organizations who maintain the technology, maintain the day-to-day security processes and influence the security culture of their organizations. In this report, we present a methodology we have developed for Measuring Information Security Maturity in Norwegian and Indian MSME's with special focus on people factor and presents the finding of the surveys. The methodology supports the measuring process by defining the parameters for diagnosis in phase 1 and analyzes information security maturity in phase 2 using the three focus areas questionnaire developed, thus discovering strong and weak areas for improving managing information security, security culture and awareness in MSME's. The major findings are presented with recommendations. Overall, the findings show that Norwegian MSME's Information Security Maturity Levels are high compared to Indian MSME's .

Preface

This thesis is a final part of my Masters of Science education at Gjøvik University College. Besides the great interest in the problem itself, the choice was also based on being able to use as much of the acquired theoretical knowledge in practice and also at same time to gain experience on how to measure information security maturity levels in Norwegian and Indian MSME's organizations with special focus on people factor .

The study had major obstacles for having participants to participant in the Norwegian and Indian Surveys. I kept enormous efforts in reaching the right people for having participants participation in the survey, they use to accept me with a smile, but use to end up with no information due to various reasons, few had no interest, few people use to ignore ,few people us to skip off, few people use to be busy with them own priorities of work and so on . But the enormous support from my wife Shirisha and Dr.Bernhard M. Hämmerli has given me high level of motivation for me to work on my thesis .

My experience showed me that the best way to make my survey successful is to use my personal and professionals contacts and use their reference for a request for participation. In turn some of them have also supported me giving me more references. I contacted around 1229 companies using personal contacts and Institute of Electronic Governance, Government of Andhra Pradesh. I was also aware that many MSME's in India do not have IT or security department .So getting information on information security maturity was a major obstacle for me. The managing directors and directors were usually busy people and therefore was difficult to get in contact with. I finally managed to get answers from 3 percent out of the 1229 companies I have contacted. As I was in India during my thesis work and was not able to get in direct contact with companies in Norway , I had a concern how I will manage with the Norwegian Survey. But my supervisors have supported me to make me feel that this was not at all a concern for me. They have supported me in making a contact with the CEO of NorSIS to get in touch with right people in MSME's and few other companies details .Out of the 20 contacts of NorSIS,40 percent have answered to the survey. In turn, I have also collected 280 companies using Internet search. But that response rate was comparatively very less. I finally managed to get answers from 6 percent out of the 361 sent.

First of all I would thank Dr.Bernhard M. Hämmerli and Co- Supervisor Dr.Nils Karlstad Svendsen of Norwegian Information Security laboratory (NISLab) for supervising the planning and work of this study and for pointing me in the right directions at different phases throughout this project.

It would not have been possible for me to complete this project if my supervisors, my wife Shirisha, information security industry expert Dr.Thomas Schlienger, Mr. Tore

Larsen Orderløkken, CEO of NorSIS, Dr.P.Madhav, Director of Promotions, Institute of Electronic Governance, Government of Andhra Pradesh, India and my contact persons have not supported me. Some have helped me getting in contact with the right persons in MSME. Unfortunately I can't mention some names, but I haven't forgotten any of you. I would like to thank the participants who participated in the surveys and who gave valuable feedback to this achieve this project successfully.

Finally, I would like to thank my wife Shirisha who is pregant and family who have let me use evenings, weekends, and holidays as well to finish the work. Thank you, all!

Table of Contents

List of figures

List of tables

1 Introduction

1.1 Topic covered by the thesis

This report constitutes the documentation for the work related to the Master thesis study in Master's in Information Security at Gjovik University College / Norwegian Information Security Laboratory. Its purpose is to develop a methodology to measure information security maturity levels in Norwegian and Indian MSME's (Micro, Small and Medium) with special focus on people factor and recommend a course of actions to improve weak focus areas based on the findings.
Information Security [23] is defined as the process of protecting the confidentiality, integrity and availability of data from accidental or intentional misuse.

In the last years, Information Security with focus on people has become a major focus area for all sizes of organizations globally. Merkow & Jim Breithaupt [23] state that people, process and technology are the three pillars of security.

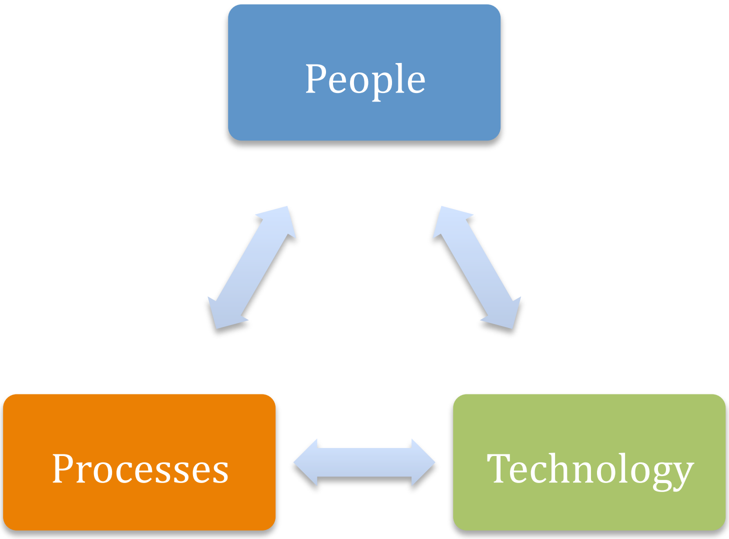


Figure 1: The People, Process and technology triad[23]

People (or employees) in organizations know that security cannot be achieved by just installing technical solutions like IDS, firewalls [18] and implementing processes. Because it is the people in turn in these organizations, who maintain the technology, maintain the day-to-day security processes and influence the security culture of their organizations. So it is important to focus on people factor to measure the security culture, security awareness and how information security is managed in these organizations.

Research on the state of information security maturity levels in different industry sectors of large organizations with focus on people, processes and technology was done by Data Security Council of India [8], Deloitte [62], Detecon [3], Devoteam

Consulting [4], Ernst& Young [9], European Network and Information Security Agency [15],KPMG [22] and Price water coopers [29].

SME's (is defined as Small and Medium enterprises) in developed countries normally have weak comprehension of information security, security technologies and control measures and so, they tend to forget about risk analysis or the development of security policies [21]. This can also be due to the fact that SME's lack the people, processes, technology and specialized knowledge necessary for coordinating information security or offering adequate information or resources on security awareness, training and education.

The level of security culture, security awareness and managing information security in MSME's varies in different countries like India and Norway due to cultural differences and people's maturity levels in these organizations. Research on the state of information security maturity level with special focus on people factors is MSME's in India is missing.

Therefore, this paper proposes a methodology that can be used to measure the information security maturity levels in Norwegian and Indian MSME's with special focus on people factor. The remainder of the report is structured as follows. In section 2, we will briefly describe the state of art on information security in SME's ,the state of research on measuring information security on people's factor, information security management, security culture and security awareness & training programs,. In section 3, we will introduce our methodology used for defining the parameters for diagnosis and measuring information security maturity levels . In section 4, we will present the survey results of Norwegian and Indian MSME's and finally in Section 5, we will conclude and give recommendations based on the findings.

1.2 Problem description

The information security in a company does not depend only on the implemented technical solutions and processes maintained in organizations. It is the people in these organizations, who maintain the technology, maintain the day-to-day security processes and influence the security culture of their organizations. Understanding this, the initial focus of this study was to measure information security awareness of employees in Norwegian and Indian MSME's before and after the security campaigns. However, it was discovered in process of discussion with industry expert Dr.Thomas Schlienger [6] that this research is out of the scope as creating security awareness and improving security culture is an ongoing process. Secondly, the same sample of participants might not be able to participate in the survey before and after security awareness campaigns, which may mislead the survey results. Therefore, after discussing with my supervisor Dr.Bernhard Haemmerli about the scope of the topic .We have agreed to narrow down the scope of project to "A Methodology for measuring information security maturity in Norwegian and Indian MSME's with special focus on people factor". After narrowing down the scope of the topic, this report also helps us to answer the following questions,

1. Write about State of research on Information Security in MSME's and State of research on Measuring Information Security on People Factor , Information Security Management, Security Culture and Security awareness & training programs
2. A Methodology for Measuring Information Security Maturity in organizations with special focus on people factor
2. Make a survey using the Methodology in Norwegian and Indian MSME's.
3. Compare the results of both regions
4. Evaluate the results and propose recommendations based on findings.

1.3 Justification, motivation and benefits

Most MSME's (Micro, Small and Medium Enterprises) today have weak comprehension of security technologies, maintaining security processes and managing information security. Secondly, people or employees in these organizations are those who take care of technology, manage day to day security processes, influence the environment or manage security in their organizations. So it is important to focus on people factor to understand the maturity levels of Norwegian and Indian MSME's organizations with respect to the security culture, security awareness and how information security is managed in these organizations. A good organization capability to remain secure is important and something that must be built. We, therefore wish to measure the information security maturity levels of Norwegian and Indian MSME's with special focus on people factor. The findings of this report can also be used as a heath indicator for creating security awareness in MSME's organizations and use it for future benchmarking.

Stakeholders for such Measurement would typically be Managing Directors/Director, Chief Information Security Officers, security managers, people working in information security office, General Managers, Information Technology Executives or employees in micro, small, medium companies in Norwegian and Indian Companies.

1.4 Research questions

To measure information security maturity levels in Norwegian and Indian MSME's with special focus on people factor is not known at the initial stage of this project, So we have come with the following research questions,

1. What is the State of Information Security in MSME's?
2. How do organizations measure information security maturity levels with special focus on people factor?
3. What is the State of research on ,
   - Information Security Management

- Information Security Culture
- Information Security Awareness and Training Programs
  - Raising the Level of Security Awareness
  - Measuring Information Security Awareness
  - Metrics for Measuring People Factor
  - Making an Effective Security Awareness Campaign

To answer all these questions we will have to have a close look at what has already been done in this area in the state of art section.

1.5 Delimitations

The focus of this measurement study is limited to Norwegian and Indian MSME's.The survey questionnaire is distributed to the respondents in India between August 1st and October 23rd 2010 and October 1st to 23rd October in Norway. The results will compared as of 23rd October survey results for both Norway and India and not with equal participants results in Norway and India as both regions were not started at the same time. The state of art collected or literature used is confined mainly to English language, as I am not aware of Norwegian language. Taking the time factor, the report will be confined only for measuring information security maturity levels with focus on people factors by taking feedback only from individuals in MSMEs. The research information available on SME's is assumed as relevant information for MSME's.

1.6 Data collection

Our research and key findings consist of electronic published articles on internet, research done by industry experts and market survey reports by Forrester Research, Ernst& Young, Deloitte, KPMG, Price Waterhouse Coopers, Data Security Council of India, European Network and Information Security Agency and among others mentioned in the bibliography.

1.7 Definitions

1.7.1 Information Security

According to Mark Merkow, Jim Breithaupt [23], Information Security is defined as the process of protecting the confidentiality, integrity and availability of data from accidental or intentional misuse.

1.7.2 Information Security Maturity

According to Suhazimah Dzazali [30], Information Security Maturity is the measurement of the organization's capability to remain secure. Here in this report for Measuring Information Security Maturity, we measure how information security is managed, security policies implemented, present status of security culture and security awareness & training programs .

1.7.3 Information Security Management

According to Mark Merkow, Jim Breithaupt [23],Information Security Management is defined as the process of managing day to day security work, training and awareness of security programs and how compliance to security policies are handled. Others areas addressed within Security Management are activities related to information classification, risk management concept and techniques, and security roles and responsibilities to assure ongoing organizational security consciousness.

1.7.4 Information Security Culture

According to Dr.Thomas Schlienger and Stephanie Teufel [32], Information Security Culture is defined by defining Organisation Culture,
Organization culture is defined how an employee sees the organization. It is collection phenomenon that grows and changes over time and, to some extent, it can be influenced by the management. Organizational culture has different subcultures based on sub organizational or functions. **Information security culture** is a subculture in regard to general corporate functions. It should support all activities so that information security becomes a natural aspect in the daily activities of every employee.

1.7.5 Information Security Awareness

According to Information Security forum (ISF) [17], Information security awareness is the degree or extent to which every member of staff understands the importance of information security, the level of information security appropriate to the organization and their individual security responsibility.

1.7.6 Effective Security Awareness

According Information Security forum (ISF) [17],**" Effective security awareness "** is defined as an ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organization from lasting behavioral change. " This definition comprises four key elements, which are shown in the figure below,

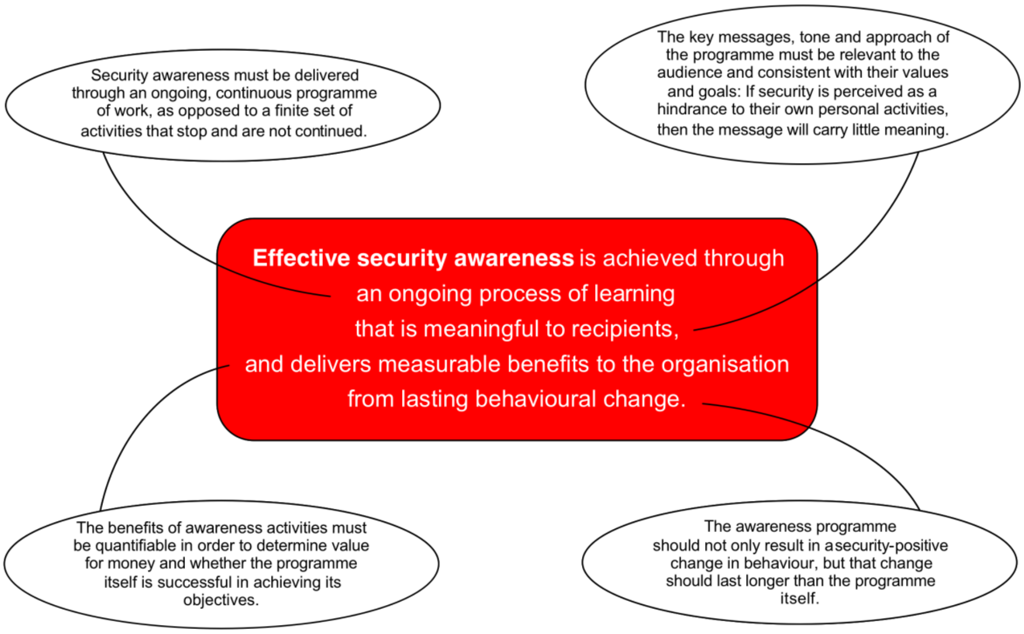

Security awareness must be delivered through an ongoing, continuous programme of work, as opposed to a finite set of activities that stop and are not continued.
The key messages, tone and approach of the programme must be relevant to the audience and consistent with their values and goals: If security is perceived as a hindrance to their own personal activities, then the message will carry little meaning.
Effective security awareness is achieved through an ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organisation from lasting behavioural change.
The benefits of awareness activities must be quantifiable in order to determine value for money and whether the programme itself is successful in achieving its objectives.
The awareness programme should not only result in asecurity-positive change in behaviour, but that change should last longer than the programme itself.

Figure 2: Effective Security Awareness[17]

According to NIST [26] . Awareness, Training and Education is defined as,
Awareness: Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities the learner is a recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate job performance.

1.7.7 NorSIS

The Norwegian Centre for Information Security (NorSIS) [28] is an organization supported by private organizations and government for coordinating activities related to ICT security in Norway. The primary target group of NorSIS is the small and medium enterprises and the public authorities. NorSIS reaches its objectives through: making the public aware of the importance of information security by means of training and information; compiling of guidelines and tutorials to help solve specific problems; and establishing an overall awareness towards information security.

2 Review and state of art

2.1 Information Security in MSMEs

What is the State of Information Security in MSME's ?

According to Dojkovski Sneza,Sharman,Waren [5][21].MSME's in developed countries generally have a weak understanding of information security management, security technologies and control measures, and neglect to carry out risk assessments or develop security policies. This may be because MSME's lack the funds, time and specialized knowledge to coordinate information security or offer adequate information security awareness, training and education.MSME's owners are not supportive of information security in terms of budget or time, thus impacting the level of security awareness and security technology. They also further point out that they are lacking specialized knowledge of security technologies, MSME's often retain the security technologies with which they are already familiar .

2.2 Measuring the State of Information Security with focus on People Factor

In this part, the research on measuring the state of information security is presented. This research has helped me for narrowing down the focus areas on the people factors and preparing the questionnaire.

To measure the level of Information Security in large companies consulting companies like Deloitte [2],Ernst& Young [9], Forrestor Research [19][20], KPMG[22],Price Water Coopers [29] has done a number of surveys globally every year taking feedback from large and multinational organizations. European agencies or organisations like Detecon [3], devoteam [4] ENISA [11] has done surveys for the European market specifically. Data Security Council of India [14] along with KPMG has done a survey to measure the maturity levels in Indian Industry.
According to publication by ENISA (European Network and Information Security Agency) on Dr.Thomas Schlienger [12] ,Security Culture improves the security level of the whole organization. Potential losses by cyber attacks, computer abuse and industrial espionage can be prevented. A good security culture should support all activities in such a way that information security becomes a natural aspect of the daily activities of every employee . Dr.Thomas Schlienger has developed a model "how can a good security culture be fostered and awareness be raised?"

How to Manage

According to ENISA [12] and Dr.Thomas Schlienger [6], Information Security Culture, like organizational culture, cannot be created once and then used indefinitely without further action or modification. It must be maintained or modified continuously. It is a never ending process, a cycle of analysis and change.

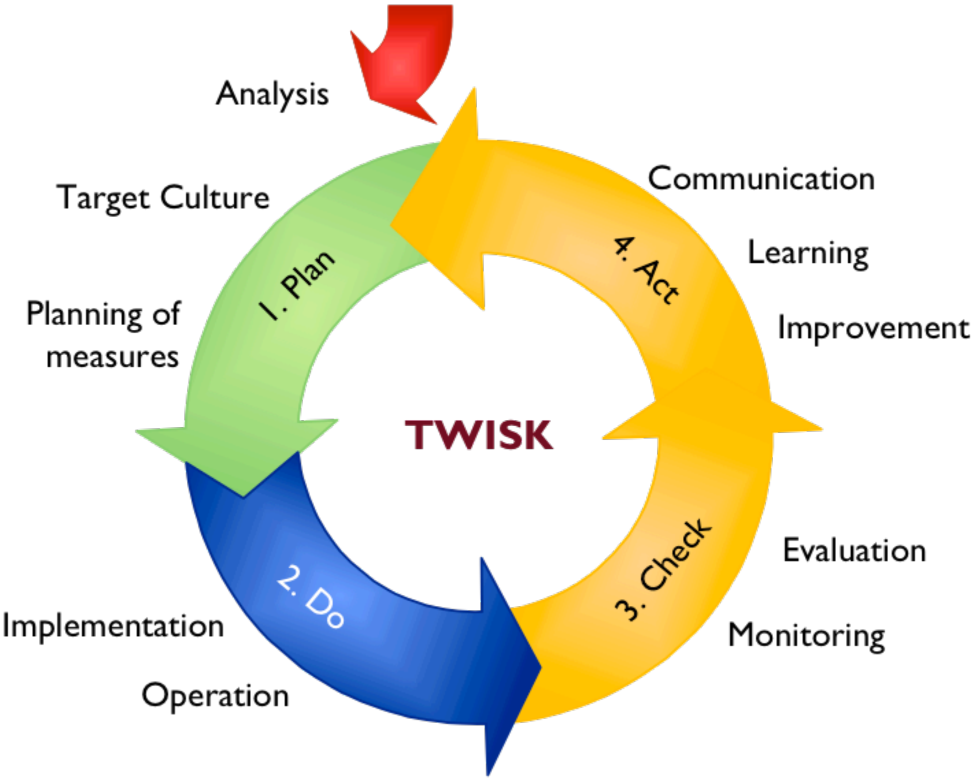


Figure 3: Information Security Culture Assessment Process[6][12]

In the process model presented by Dr.Thomas Schlienger, the first step is to analyze the actual information Security Culture (assessment). If the culture does not fit with the organization's targets, the culture must be changed. If it fits, it should be reinforced. The necessary actions must be chosen (planning) and realized (implementation). The success of the actions taken must then be checked and learning is specified (evaluation).

How to measure

Dr..Thomas Schlienger have a set of methods for measuring security awareness and culture . One of the main contributions of Dr.Thomas Schlienger research work was the development of an analysis framework to measure the level of security culture.

Understanding the difficulties in different culture. Dr.Thomas Schlienger has also developed a standardized questionnaire on the basis of an organizational behavior model, which is integrated in an assessment tool. The tool measures the three layers of organizational behavior: organization, group and individual, with in all below twenty areas (e.g. work and technology design, communication, attitude etc.) as in the figure.

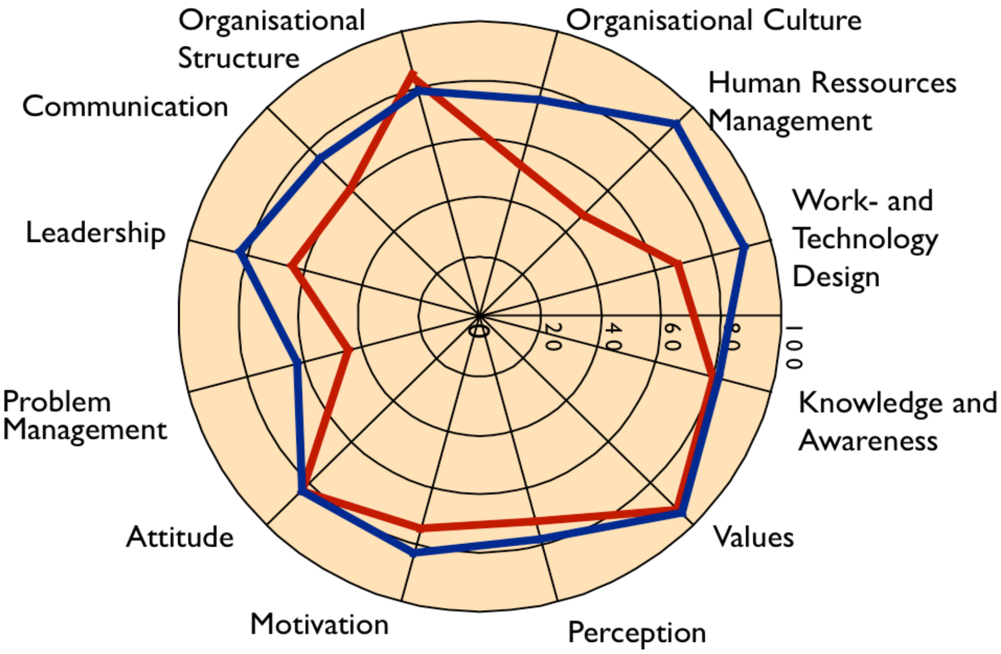
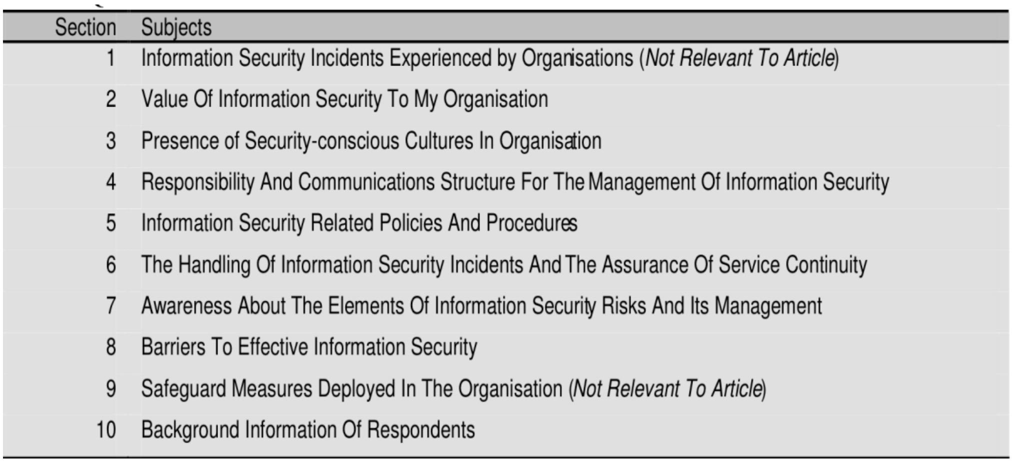


Figure 4: Information Security Culture Radar [6][12]

The tool allows comparison of the Information Security Cultures between different organizations (benchmarking) or that of a Culture within the same organization over different points in time. This method and tools helps to bridge this gap by allowing organizations to systematically analyze their information security culture, to quickly identify weaknesses and improvement actions and to prove progress in Information Security Culture. This tool also helps to support the advantage of shorter project cycles, higher work quality processes and best practices, less resources (time, budget, manpower) and leads to a sustainable improvement in the security culture.

Suhazimah Dzazali [30] has done an empirical study to measure the information security maturity and social factors of an organization. The questionnaire was structured based on the below 10 subjects from section 1 to section 10.This emphirical study by Suhazimah Dzazali helps in preparing the questionnaire on the focus areas in this thesis work.



Section	Subjects
1	Information Security Incidents Experienced by Organisations (*Not Relevant To Article*)
2	Value Of Information Security To My Organisation
3	Presence of Security-conscious Cultures In Organisation
4	Responsibility And Communications Structure For The Management Of Information Security
5	Information Security Related Policies And Procedures
6	The Handling Of Information Security Incidents And The Assurance Of Service Continuity
7	Awareness About The Elements Of Information Security Risks And Its Management
8	Barriers To Effective Information Security
9	Safeguard Measures Deployed In The Organisation (*Not Relevant To Article*)
10	Background Information Of Respondents

Table 1: Subjects areas[30]

2.3.1 Information Security Management (ISM)

According to Alnatheer,Mohameed and Nelson [25] ,ISM standards are used to establish and maintain a secure environment for information. ISM help senior management to monitor and control their security, thus minimizing any business risk and ensuring that security continues to fulfill corporate, customer, and legal requirements . The overall goal of ISM is the prevention or minimization of damage to organizational assets. ISM can enhance organizations' performance, and its establishment in the normal way of doing business . They also state that information security and its management are concerned with people, processes and technology and the technology itself can be seen as relatively objective by nature; the people and processes are influenced by the environment in which they operate.As mentioned [23],ISM is defined as process of managing day to day security works,training and awareness of security programs and compliance to security policy. Alnatheer,Mohameed and Nelson [25] has also stated that Information security policy helps to define the users' rights and responsibilities in terms of information within an organization. Effective information security policies will help users understand what is acceptable and responsible behavior in information resources and will assist in establishing a safe information environment. Information security policy is an essential part of security practices within organizations and could substantially influence on their organizational security. "Without a policy, security practices will be developed without clear demarcation of objectives and responsibilities", and will face major difficulties when implementing ISM System effectively in their organizations' infrastructures. As a result, organizations cannot achieve effective ISM system without the establishment, implementation, and maintenance of an information security policy. In addition, the formulation and utilization of information security policy can enhance the effectiveness of ISM system.

2.3.2 Information Security Culture

Experts have previously proposed conceptual frameworks for information security management that includes information security cultural development based on management initiatives of policy, awareness, training, and education [5] . In recent years, several dedicated frameworks for information security culture have emerged, based on: organizational culture and the measurement of information security culture[32] at individual, group and organizational levels of information security .

2.3.3 Information Security Awareness

In this part, the research on information security awareness, various channels of raising security awareness, measuring information security awareness, metrics and effective security awareness and campaigns process is presented in below sections,

2.3.3.1 Information Security Awareness and Training Programs

According to Alnatheer,Mohameed and Nelson[25] ,Employee's gain an understanding of appropriate IS culture and practice through awareness raising and training programs.Information security awareness is important part of ISM . Increasing awareness of security issues is the most cost-effective control that an organization can implement . however suggests that the absence of awareness programs indicate a critical gap in effective security implementation. Security training and awareness programs are therefore a fundamental component of effective information security strategy. Security awareness and training can help organizations to minimize some of the damage caused by misused or misinterpreted application procedures .Information Technology Security Training Requirements: A Role and Performance Based Model by NIST publication 800-16 [24] has presented a learning process how awareness, continues into training and evolves into education.

2.3.3.2 Raising the Level of Security Awareness

In this part, the research on how organizations can raise the level of security awareness is presented. This research has helped me to define the answer options for the question of security awareness.

David Lacey [1] in " Managing the Human Factor in Information Security 2009" presented a variety of channels like email, web pages, newsletters, journals, images, flyers, posters, competitions and presentations to raise awareness and communicate the messages in an effective way. In addition, he also states that professional supporters like copywriters, technical writer, marketing experts, and behavioural psychologists can also make substantial difference for an effective campaign. Modern channels such as blogs are becoming essential channels for disseminating information in an interactive process. But he also mentions that before designing an effective campaign, information about what people know and think about the subject and

behave is very important process to analyse and then raise an effective campaign process.
ENISA [10] in " the new users guide: how to raise information security awareness " presents some channels like the brochures, magazines, comic, distance learning, education, emails, events, newsletters, newspapers, phone, posters, radio, screensaver, SMS, training, TV, Videos and websites, which can help to raise the level of awareness. They also state the advantages and disadvantages of using these channels for raising awareness in organizations

Channel	Advantages	Disadvantages
Brochure or Magazine	Easier to define message content and format Allows for careful study of content by Target group Established audiences can be reached	Not a static source of information as material could be cost May only appeal to a select target group
Comic	Instant appeal to certain target groups like the young Message content can be more attract in nature	Difficult to incorporate messages with more detail May only appeal to a select target group
Distant learning -computer based training(CBT) -Online Training	Enables training over geographically disappeared areas Message content can be more detailed	Can be expensive to create training programmes Implies trainee has some technical knowledge already
Education -Education pack -Teaching material	Good way to reach large numbers of children Often established channels exist to distribute materials	Time in school is already at a premium and curricula are often crowded Teachers may not have expertise to deliver message Computing facilities may not allow some activities e.g. Practice in installing antivirus software
Email	Relatively cheap channel to target mass audience Allows target group to digest information in own time	Message may be undermined due to volume of emails and spam Email addresses must be known
Event -Fair	Can reach a very wide range of audiences by careful selection of venues and topics	Your intended audience may not attend Not a proactive channel with

-Meeting **-Seminar** **-Conference**	Has more chance of interesting the audience due to the interactive element of the channel	target group expected to participate
Leaflet or Factsheet	Can provide a lot of information Cost effective to produce	Need to organize distribution channels so your leaflets get the right audience Not a static source of information as material could be lost
eNews letter	Have similar advantages as with the email channel	Not a proactive channel as typically requires users to register Implies trainee has some technical knowledge already
News Paper	Mass circulation with deep market penetration. On a cost per thousand basis, Newspapers are generally inexpensive cost-effective means of delivering a message to a wide audience A newspaper ad gives as much Detailed information as is needed and even display imaged or logos	The clutter factor, There is a lot of competition for the reader's attention in a newspaper. Newspapers are usually filled with many ads, in various sizes and styles, promoting many products and services If wishing to reach only a specific population segment may find that newspapers waste too much circulation Newspapers have a short life, they are frequently read in a rush, with little opportunity for careful study
Phone	Allow direct target group contact Has more chance of interesting the audience due to the interactive element of the channel	Can be relatively expensive Target group contact details need to be available
Poster	Can be attention grabbing due to size and format Information can be universally available when put up on walls	With abundance of information material, message may be over looked
Radio	Radios biggest advantage is high frequency (reaching the same audience numerous times) at a reasonable cost Station music formatting helps define interest groups	Radio has heavy commercialization You cannot show your subject and cannot demonstrate it A radio spot lacks the permanence of a printed message

	and some demographic categories. So you can choose the specific type of audience you'd like to reach	Because of formatting and audience specialization, a single station can seldom offer broad market reach
Screensavers	Places information on the computer so users are likely to see it	Requires development Inexperience users may be unable to install it Does not reach those without computers
SMS	Message content can be delivered straight to the target group ensuring visibility	Need to work with telecoms provider Effective channel to alert the target group of dangers but not raise awareness due to limited content
Training	Has more chance of interesting the audience due to the interactive element of the channel Content of message can be more detailed and customized	Not a proactive channel with the target group expected to participate Can't really reach mass audience due to resources and logistics involved
TV	High impact, Combining sight, sound and motion- can be attention getting and memorable TV comes as close as any medium can face-to- face communication The personal message delivered by an authority can be very convincing You can demonstrate message TV offers audience selectivity by programming. It offers scheduling flexibility in different programs and day parts and opportunity to stress reach or frequency	Cost-budget requirements are relatively high Although you can pick your programs, you run the risk of the most popular shows being sold out
Video **-DVD** **-CD**	Allows for creative freedom with awareness message Professionalism of channel if implemented correctly could	May not reach a technologically naïve audience

	help enforce message	
Website	Can be updated to reflect changes Can present content for multiple audiences Can easily link to other information	May not reach a technologically naïve audience Implies trainee has some technical knowledge already Not a proactive channel and with and with wealth of websites and information on the internet available, message may get overlooked

Table 2: Channel of Communications with advantages and disadvantages[10]

2.3.3.3 Measuring Information Security Awareness

In this part, the research on how organizations can measure the level of security awareness is presented. This research has helped me to understand the various ways of doing a measurement study and for developing the methodology for measuring information security maturity levels in organizations with focus on people factor.
Mr. Johnny Mathisen[18] in thesis has stated, some ways for measuring the level of security awareness,

- Internet based questionnaire is one of the best way to make statistical analysis to measure the information security awareness from a large pool of employees or people. Most of the Multinational and Transnational companies prefer to do this kind of survey quarterly to measure the awareness levels.
- Paper based questionnaire is another tool used by smaller companies for measuring employees awareness .The collected data from this questionnaire can also fed to the internet based questionnaire manually to get a statistical report.
- Personal interviews normally take longer time compared to the others tools. But this form helps to go deeper into the subject and get some key findings, which is normally not given in Internet based surveys.
- Group discussions and workshops can be another form for measuring awareness. But this is mainly a matter of getting resources and makes large people to participate in such discussions.

A prototype for assessing information security awareness by H.A Kruger and W.D Kearney [16] presents a measuring tool to measure the information security awareness levels at each region. This model measures on three dimensions mainly, what does a person know (knowledge); how do they feel about the topic (attitude); and what do they do (behaviour) and six focus areas which the management feels necessary. This tool helps to measure the knowledge, attitude ,behaviour and assists in providing feedback to the management about the success of the information security awareness programme.

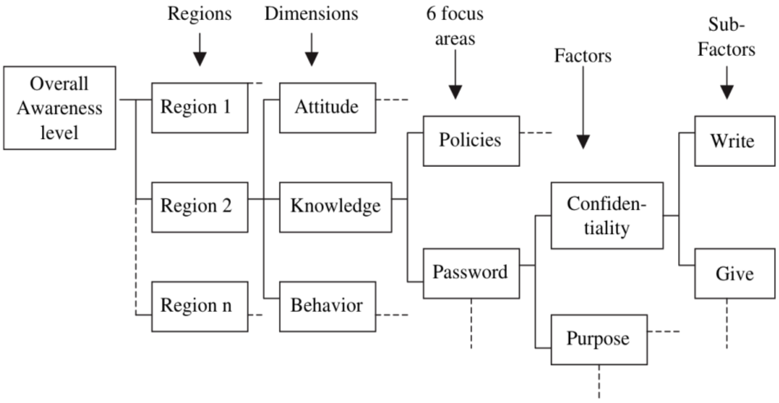


Figure 5: Tree structure" prototype for assessing information security awareness[16]

2.3.3.4 Metrics for Measuring People Factor

In this part, the research on metrics on measuring people factor is presented. This research has helped me in developing the questionnaire taking the below metrics as a base line.

ENISA [10] stated metrics that are proved to be effective at measuring the success of information security awareness activities like number of security incidents due to human behaviour, audit findings, results of staff surveys, tests of staff follow correct procedures, number of staff completing training, qualitative feedback from staff, costs of security incidents due to human behaviour, number of visitors visiting the security intranet site and proportion of downtime due to human behaviour. A example of a survey question asked by ENISA to know which metrics are proved effective at measuring the success of information security awareness activities is presented below,

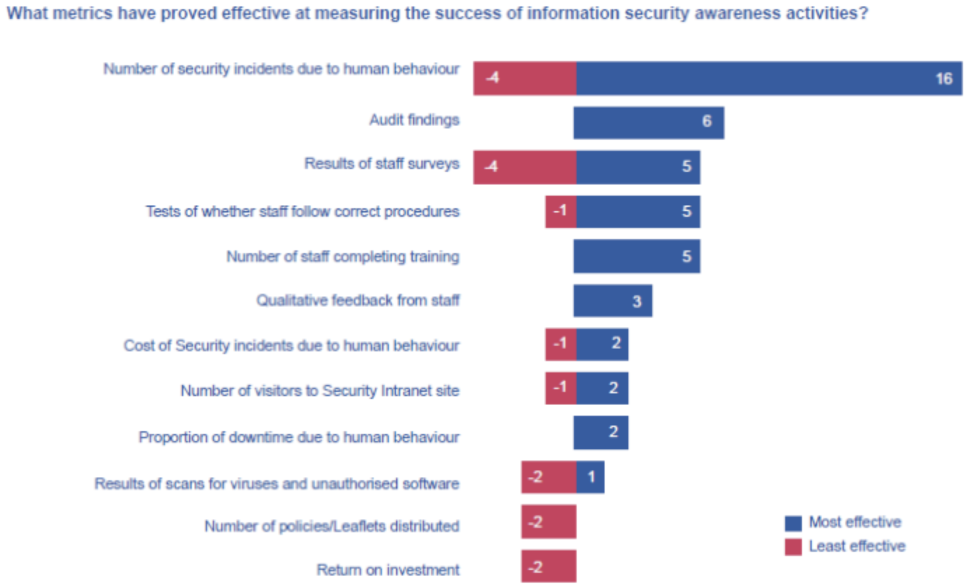


Figure 6: Metrics for Measuring Information Security Awareness[10]

NIST in 2003 [26] has also released "Security Metrics Guide for Information Technology Systems" with some examples. "Effective Security Report "[17] by ISF forum statemetrics that are used to measure the success of the campaigns before and after the campaigns. ISF used these metrics to compare the change in behaviors before; during and after the awareness campaign are run.

Awareness theme	Examples of metrics
Feedback from staff	• Number and timing of visits to security intranet pages • Number of queries about security-related issues • Number of incidents reported by staff (as opposed to discovered by the security team) • Response to security newsletters, surveys, competitions • Delayed measurement of awareness (knowledge, attitude, behavior) – leave for a month after training to see if the message has 'stuck'
Incidents	• Frequency and severity of major incidents and frauds, and cost of resolving • Number, severity and source of virus incidents, and resulting downtime • Number of 'repeat' incidents (i.e. recurrence of a previous problem)
Internet/e-mail misuse	• Quantity and severity of blocked inbound and outbound e-mails • Balance of business vs. personal Internet use, access to blocked sites • Type and volume of file downloads
Password management	• Password strength (e.g. use password crackers such as lophtcrak) • Password resets (analyze cost of resets, worst departments)
Physical security	• Clear desks: locked drawers, locked workstations (clear screens), with photographs of the findings • 'Tailgating': monitoring staff admitting others without security passes • and challenging them immediately to make them aware of the problem • Number of temporary passes issued to a) visitors and b) staff each day, and number of these that are returned • Quantity/value of laptop thefts
Security management	• Risk analysis scores (e.g. Information Security Status Survey) • Percentage of systems development projects that

	undergo a formal risk analysis during the design phase • Number of derogatory mentions of company from Internet scans
System management	• Timeliness of patches and security fixes • Number/privileges of redundant/unused/generic (e.g. 'guest') accounts • System downtime, causes, engineer activities • Percentage of system changes that go through a formal change process • System configuration
System misuse	• Unauthorized or personal files (e.g. .mp3, .jpg, very large files) on • storage media • Software license audit

Table 3: Awareness Metrics[17]

2.3.3.5 Making an effective security awareness campaign

In this part, the research on making an effective security awareness campaign is presented. This research helps MSME's organizations to know how effective security awareness campaign can be created based on the findings of survey results in this report.

In the publication by NIST 50[26] of 2003 "Building an Information Technology Security Awareness and Training Program" presents a model for building an effective IT Security awareness and training program. It also explains the inter relationship between awareness, training and education .It starts with awareness, builds up to training and evolves into education

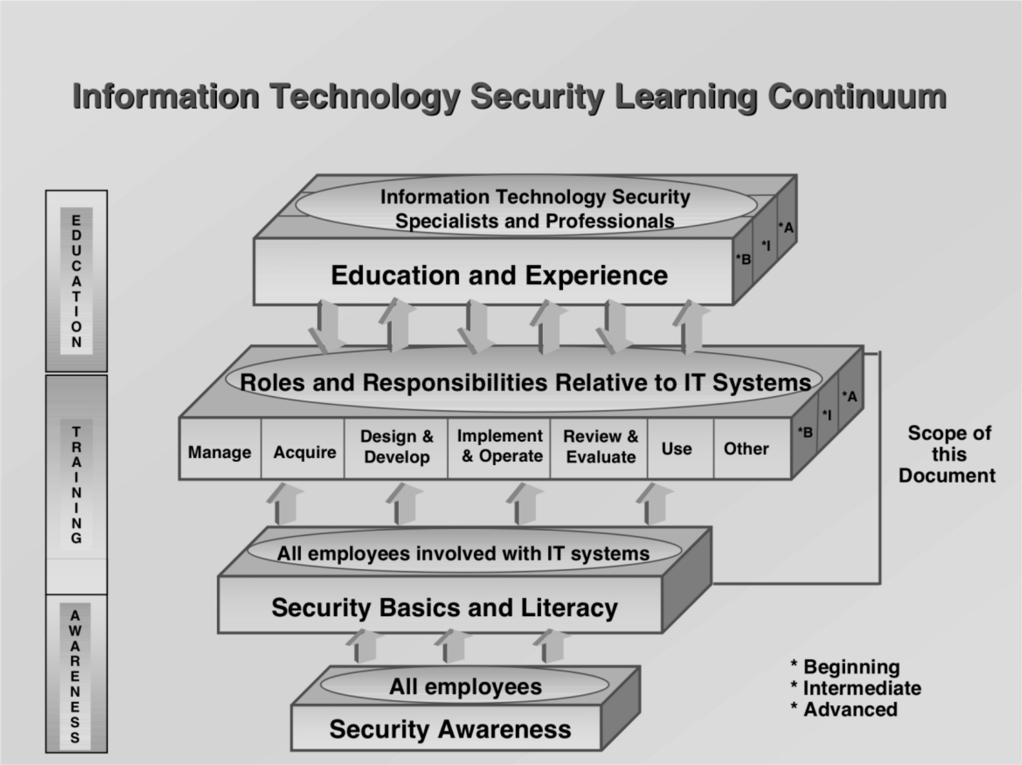

Information Technology Security Learning Continuum
EDUCATION
TRAINING
AWARENESS
Information Technology Security Specialists and Professionals
Education and Experience
*B
*I
*A
Roles and Responsibilities Relative to IT Systems
Manage
Acquire
Design & Develop
Implement & Operate
Review & Evaluate
Use
Other
Scope of this Document
All employees involved with IT systems
Security Basics and Literacy
All employees
Security Awareness
* Beginning
* Intermediate
* Advanced

Figure 7– IT Security Learning Continuum[26]

The model is role-based and defines the IT security learning continuum a person needed assuming the different roles and responsibilities within an organization in relation to IT systems. This document uses the model to identify the knowledge, skills, and abilities an individual needs to perform in the IT security responsibilities specific to each of his or her roles in the organization. The type of learning that individuals need becomes more comprehensive and detailed at the top of the continuum. Thus, beginning at the bottom, all employees need awareness. Training (represented by the two bracketed layers "Security Basics and Literacy" and "Roles and Responsibilities Relative to IT Systems") is required for individuals whose role in the organization indicates a need for special knowledge of IT security threats, vulnerabilities, and safeguards. The "Education and Experience" layer applies primarily to individuals who have made IT security their profession.

This report also presents four critical steps in the life cycle of the awareness and training process.

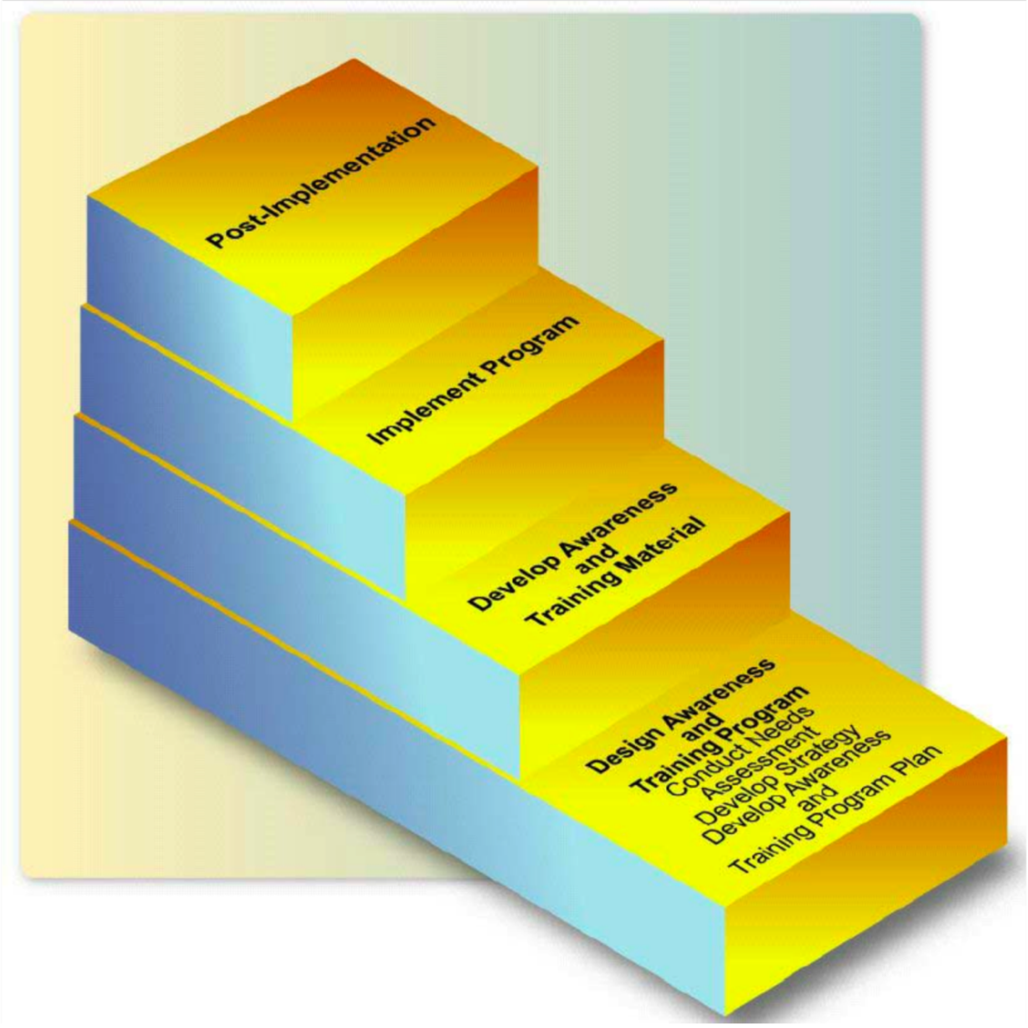

Post-Implementation
Implement Program
Develop Awareness and Training Material
Design Awareness and Training Program
Conduct Needs Assessment
Develop Strategy
Develop Awareness and Training Program Plan

Figure 8– Keys steps in the life cycle of an awareness and training program[26]

1. Designing Awareness and Training Program: - The first step in this cycle includes activities like structuring the awareness and training program, develop a strategy to achieve the goal and fund the program.
2. Developing Awareness and Training Material – Selecting the necessary topics for the campaign. For example, topics like password usage, social engineering and internet usage at office.
3. Program Implementation is a process for getting the developed awareness plan to be the target groups. It includes the process of getting the messages across to the employees through presentations, posters, newsletters, emails and screensavers etc.
4. Post-Implementation: - The last step in the process after implementation includes monitoring the effectiveness of the campaigns. The formal evaluation and feedback mechanisms play a critical role after any security awareness, training and educating program. The below figure shows a example of such evaluation and feedback mechanisms, so that post implemented can done in various ways.

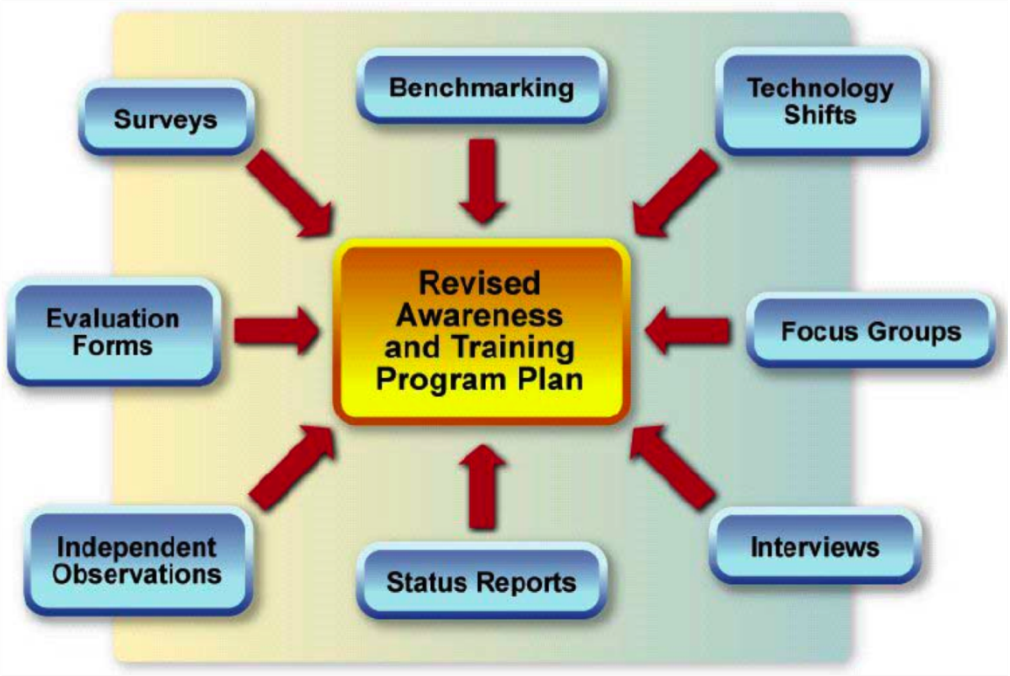


Figure 9 - Evaluation and feedback techniques[26]

ENISA [13] in " The growing requirement for information security awareness " presented a change management strategy for raising information security awareness in financial organizations .The model presents that it is an ongoing process, a cycle of analysis which must be maintained or raised continuously to have more effect. This program helps to close the gap between particular issues and human responses that need a change.

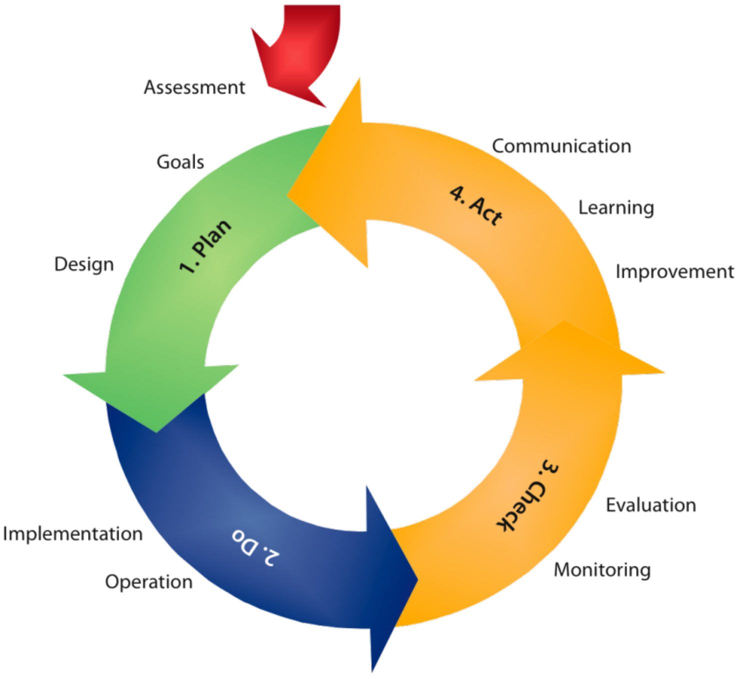


Figure 10: Overall Strategy for raising information security awareness[13]

The first step is to analyze the actual information security awareness and identify the main business drivers for the needs of an awareness programme. Once the needs are identified, the program has to be designed and reviewed for management presentation. In the next stage (implementation) a platform for delivery, assigning project resources, planning and executing the roll out has to be deployed keeping the objectives in mind. The success obtained from the implementation must be evaluated (measured) and further programme improvement has to be done as illustrated in figure above.

3 Methodology

In this part ,we present the methodology for Measuring Information Security Maturity **in** Norwegian and Indian MSME's with special focus on people actor.

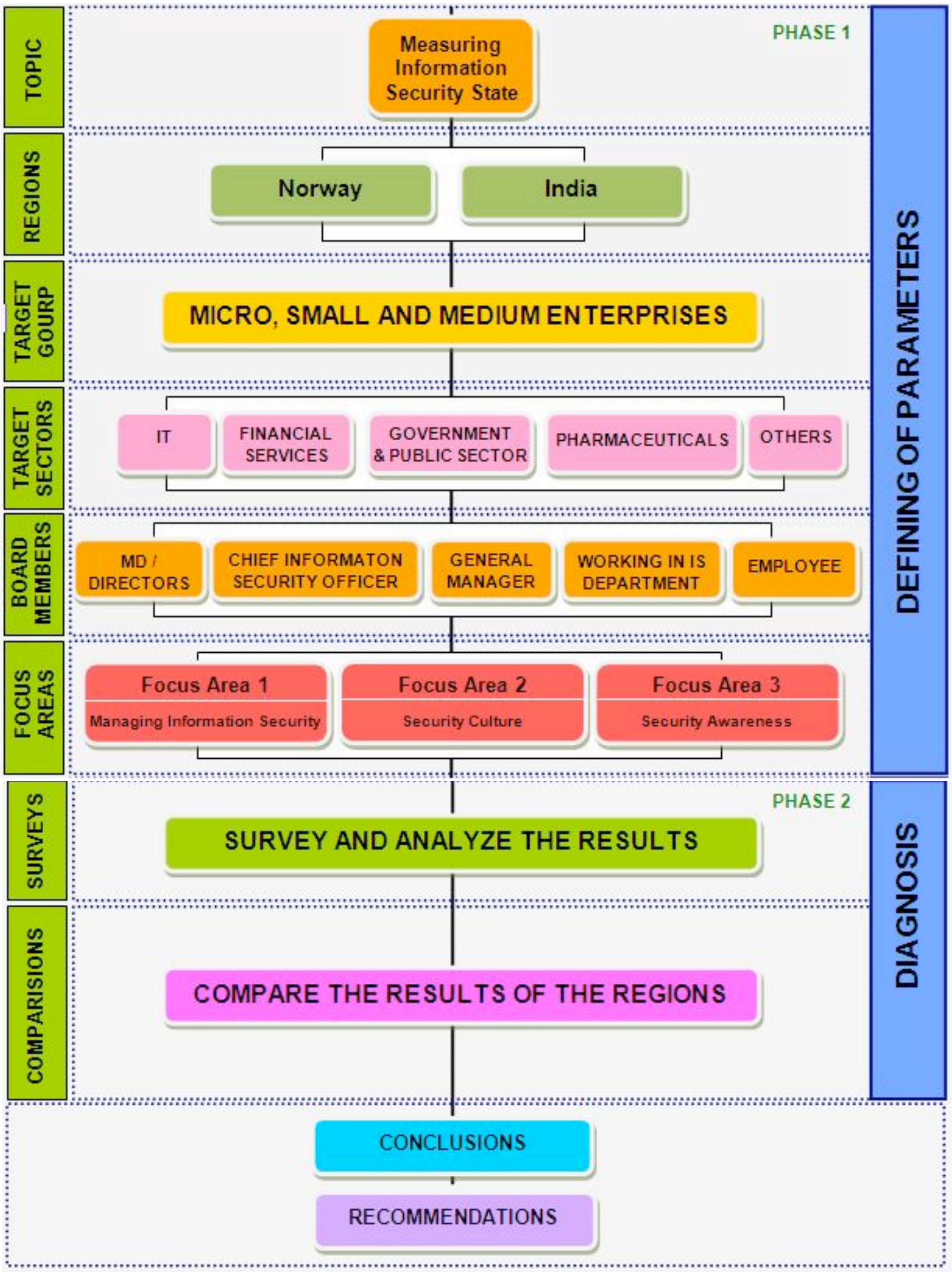


Figure 11: A Methodology for measuring information security maturity in Norwegian and Indian MSME's with special focus on people factor.

The Methodology has two phases in the measurement process,

3.1 What to measure– Phase 1

In phase one, the parameters like target regions, target groups, board members and focus areas are defined for measuring information security maturity levels.

The developed methodology is now used in measuring the information security maturity in Norwegian and Indian MSME's targeting the survey participants from IT, Financial Services, Government & Public Sector, Pharmaceuticals and other industry sectors as the main target sector participants.

Normally defining focus areas is based on the requirement of different regions and target groups measurement requirements, but in this report in order to measure the maturity levels of the Norwegian and Indian MSME's with special focus on people factor ,we have used managing information security, security culture and awareness as the main focus areas for the preparation of questionnaire.

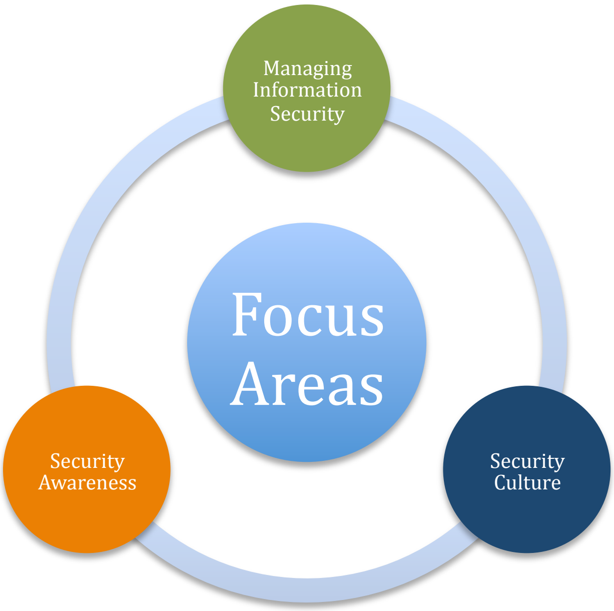


Figure 12: Focus areas

The questionnaire developed was prepared based on the survey questionnaire prepared by Deloitte[6], Detecon[3] ,Devoteam Consulting [4] ,Data Security Council of India cooperation[8],Ernst& Young[6], Dr.Thomas Schlienger of Tree Solution [7] ,Forrester Research [19], European Network and Information Agency [11] ,KPMG[22] and Price water coopers [29] for measuring information security state in large enterprises with focus on people, processes and technology. Mainly questions from "Survey from Information Security Culture "[12],Ernst Young 2009 [16] ,“ Awareness Raising Quiz templates for parents, end users and SME “[18] by ENISA and “The State of SMB IT Security Market and Emerging Trends: 2009 to 2010 “[31] are used to prepare the questionnaire .The questionnaire prepared was mainly focusing on the people factor as people or employees in these organizations are those who maintain the technology, manage day to day security processes, influence the environment or manage security of their organizations. So it is important to focus on above people factors to understand the maturity levels of Norwegian and Indian MSME's.

Based on the focus areas, 19 questions and answer choices were developed in different formats like single choice & multiple choice answers, rating scale and matrix of choices

S.No	Section Subjects
1	Managing Information Security
2	Security Culture
3	Security Awareness
4	Background Information of Respondents

Table 4: Questionnaire Structure

In normal measurement process, the above subject areas are individual focus areas for measurement. But in this study, we use all the above focus areas and subjects for knowing the MSME's maturity levels. Further related questions on the each subject areas are asked. This process of defining the parameters for measurement in phase 1 is as a step-by-step approach, which is a simple representation of a measurement process.

3.2 How to Measure – Phase 2

The second phase of measurement process is to analyze the actual information security maturity in Norwegian and Indian SME's defined as "diagnosis" phase. The questionnaire is now sent directly to the security custodians or individuals through emails with an online link to answer the questionnaire .The participants here are basically from the senior management or middle management or operational level positions who are caretakers, decision makers of IT and Information Security issues or employees in these organizations.

The MSME's (target groups) in this measurement are contacted with support of NorSIS [28] and personal contacts .Survey with Indian MSME's is done with cooperation of Institute of Electronic Governance, State Government of Andhra Pradesh, India [33] and personal contacts. Invitation Letters are sent to these MSME's through emails with a request to participate in the survey. In addition to these emails, associations, governmental agencies and friends are contacted requesting them to support for the survey by asking them to forward this invitation to friends and cousins working in various MSME organisations for their participation.

After analyzing the results from the online survey in phase 2. A comparison study is made to compare the similarities and differences in two regions (Norway and India) with respect to information security Maturity in different industry sectors and sizes of companies. Later recommendations are recommended to the target groups to improve the information security maturity levels based on the conclusions.

The methodology is sustainable and can be applied over and over. It is fairly easy to use and output is given in a quantitative manner that is easy to understand. In general the methodology provides a number of opportunities to benefit from

- The methodology not only will measure the information security maturity in Norwegian and Indian MSME's and focus areas, but helps to define the diagnosis parameters like target regions, target groups and sectors, target levels, focus areas, analyzing and interpretation of results in a step by step simple process and for further enhancing the methodology.
- By applying the methodology at regular intervals, the change in maturity levels can be measured and an index of maturity levels can be constructed. This will assist MSME management to measure the change in maturity levels over a period time and to take corrective action if necessary.

4 Survey

4.1 About this survey

Using the developed methodology and questionnaire, we will measure information security maturity levels in Norwegian and Indian MSME's. The survey findings are presented based on the below focus areas namely; managing information security, the present status of the security culture , security awareness and training programs in MSME's.

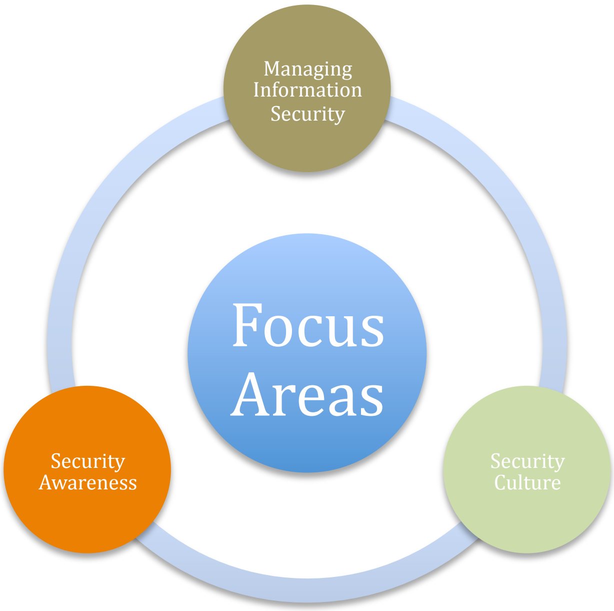


Figure 13: Focus Areas in Survey Questionnaire

In all, the survey results for the MSME's will be an aggregate data for and Norwegian and Indian participants.
Geography: Participants in the MSME survey were from Norway and India, with 33 percent from Norway and 67 percent from India.

BASIC SEGMENTATION AVAILABLE

Industry	IT	Manufacturing
	Financial Services	Leather
	Pharmaceutical	NGO
	Government &Public sector	Others (include Oil &Gas ,Inshore diving , Logistics , Healthcare , Education , Printing , Renewable Energy , Electronics & IT)

Company size (SME)	Micro	Small and Medium business
	1 to 19 employees	20 to 99 employees
		100 to 250 employees

Countries	Norway
	India

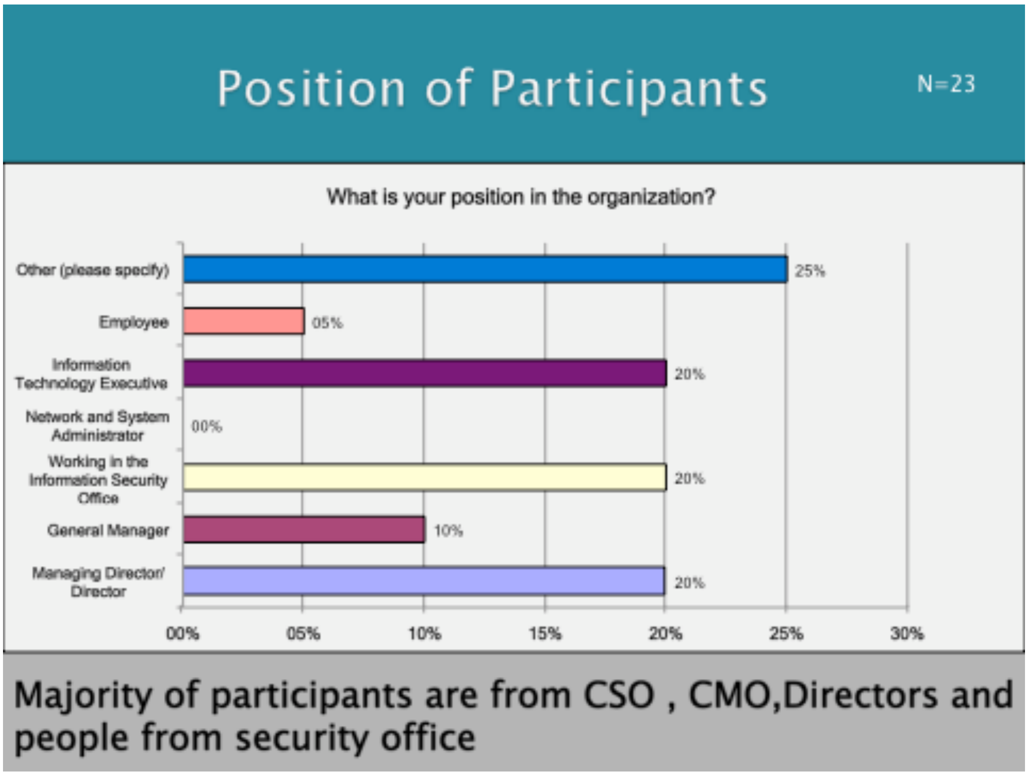
Table: 5 Segmentation on Target Groups

4.2 Company and Respondent Profile

The survey had the following breakdown between the Norwegian and Indian Organization participants:

Job title:

In the Norwegian MSME survey,20 percent of the participants were Managing Directors and Directors,10 percent of participants were General Managers, 20 percent were working in the information security office, 20 percent were information technology executives,25 percent of participants were from other category with roles like Director of Group Security , CSO and CMO etc



Position of Participants

N=23

Majority of participants are from CSO , CMO,Directors and people from security office

Figure 14: Position of Participants in Norwegian MSME's Survey

In the Indian MSME survey,51.3 percent of the participants were Managing Directors and Directors,7.7 percent of participants were General Managers, 2.6 percent were working in the information security office,2.6 percent were network and system administrators,5.1 percent were information technology executives, 12.8 percent of participants were from other category with roles like Marketing Managers etc and employees were 17.9 percent of participants.

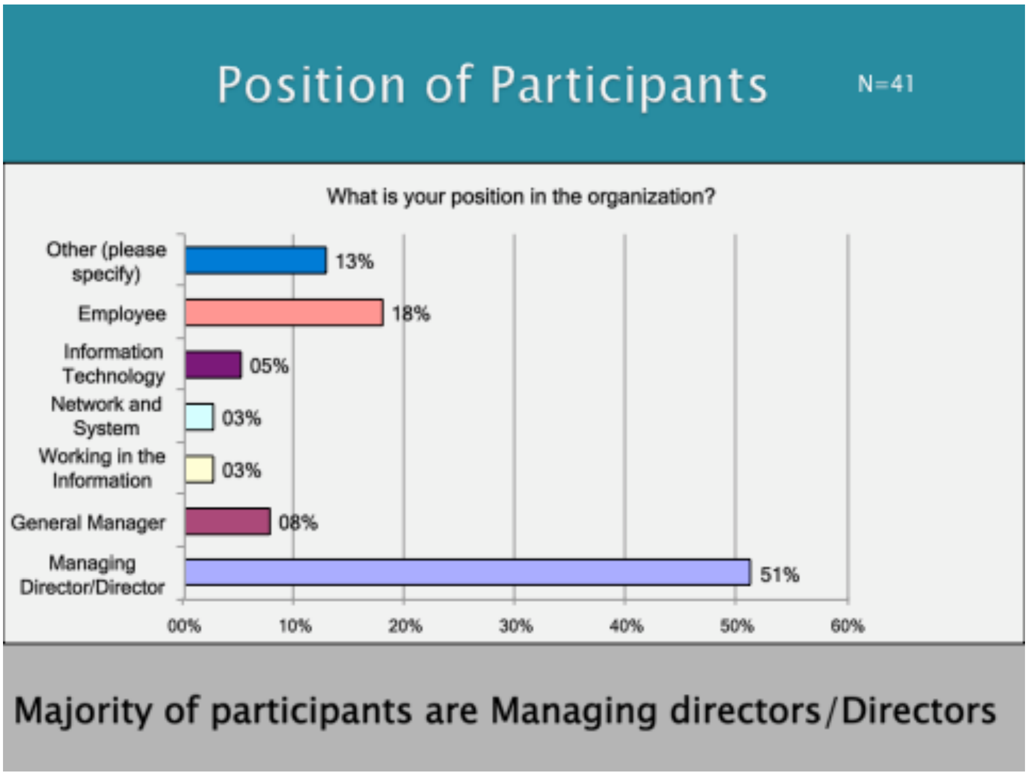
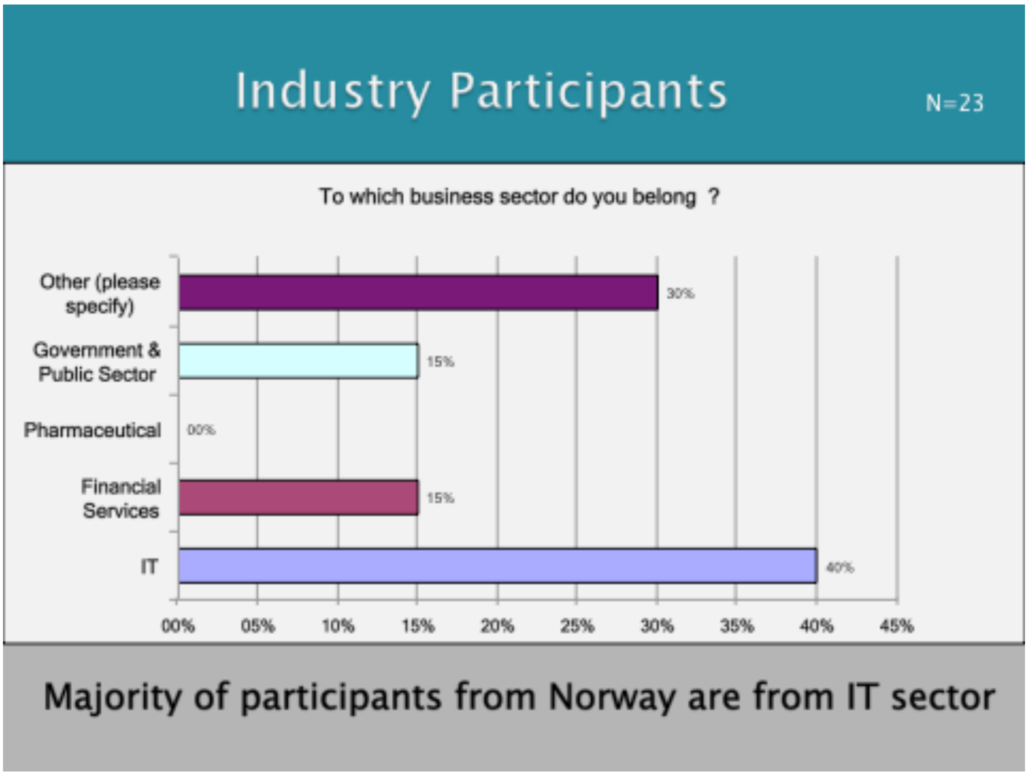


Figure 15: Position of Participants in Indian MSME's Survey

Industry: We divided the survey participants in seven industries. In the survey, the seven industries are IT, finance services , Pharmaceutical, Government & Public and Others (Which include oil & gas , inshore diving , logistics , health care , education , printing ,renewable energy , electronics &IT and leather etc).

In the Norwegian MSME Survey,40 percent are IT,15 percent were financial services,15 percent were government & public sector and 30 percent were other sector enterprises.


Industry Participants N=23

Majority of participants from Norway are from IT sector

Figure 16: Industry Participants from Norwegian MSME's

In the Indian MSME Survey, 43.6 percent were IT, 12.8 percent were financial services, 15.4 percent were pharmaceutical, 7.7 percent were governmental & public sector and 20.5 percent were other industry sector enterprises.

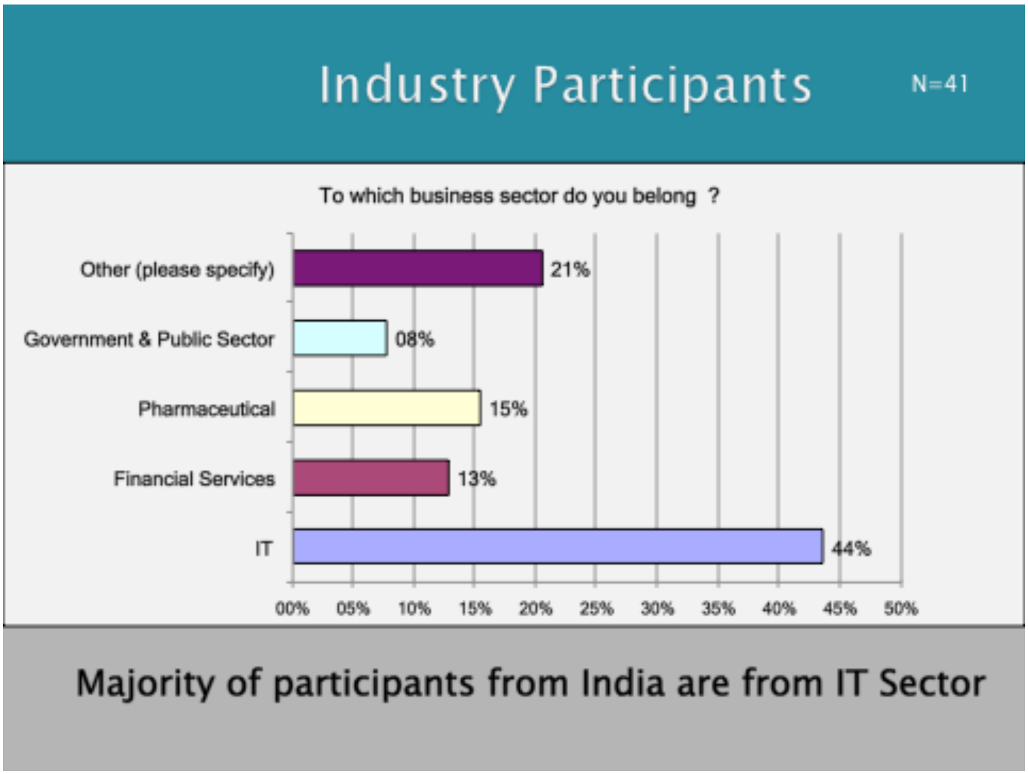
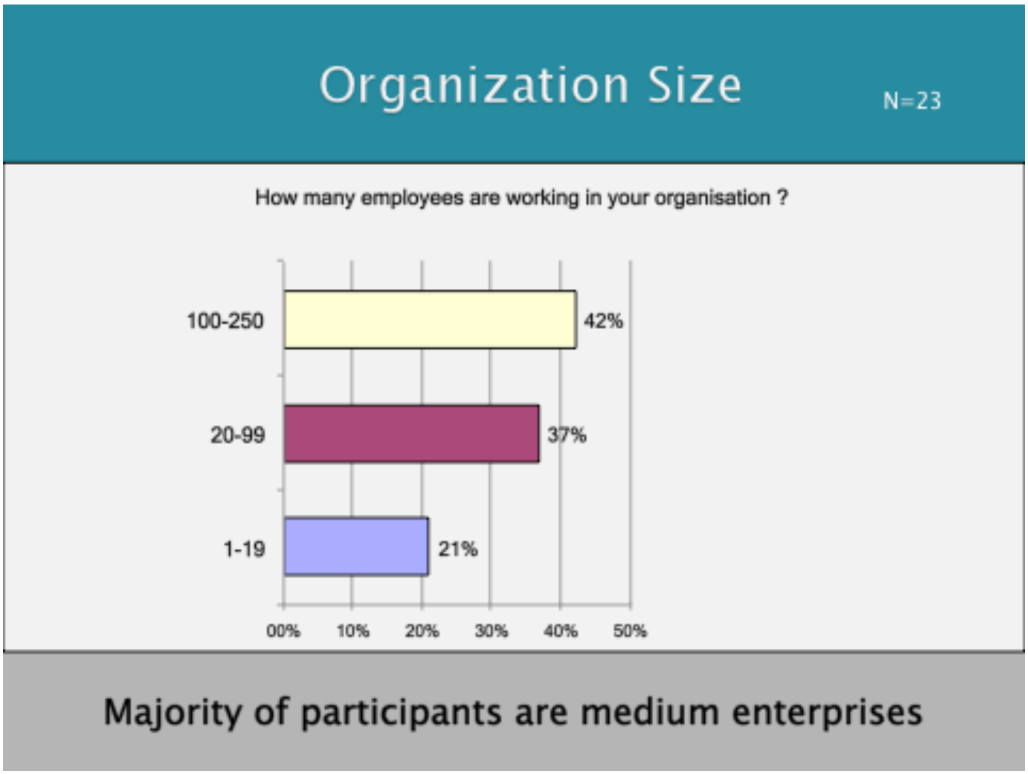


Figure 17: Industry Participants from Indian MSME's

Organization size:

In the Norwegian MSME survey, 21.1percent of participants were from companies with 1 to 19 employees, 36.8 percent of participants were from companies with 20 to 99 employees and 42.1 percent of participants were from companies with 100 to 250 employees.



Organization Size

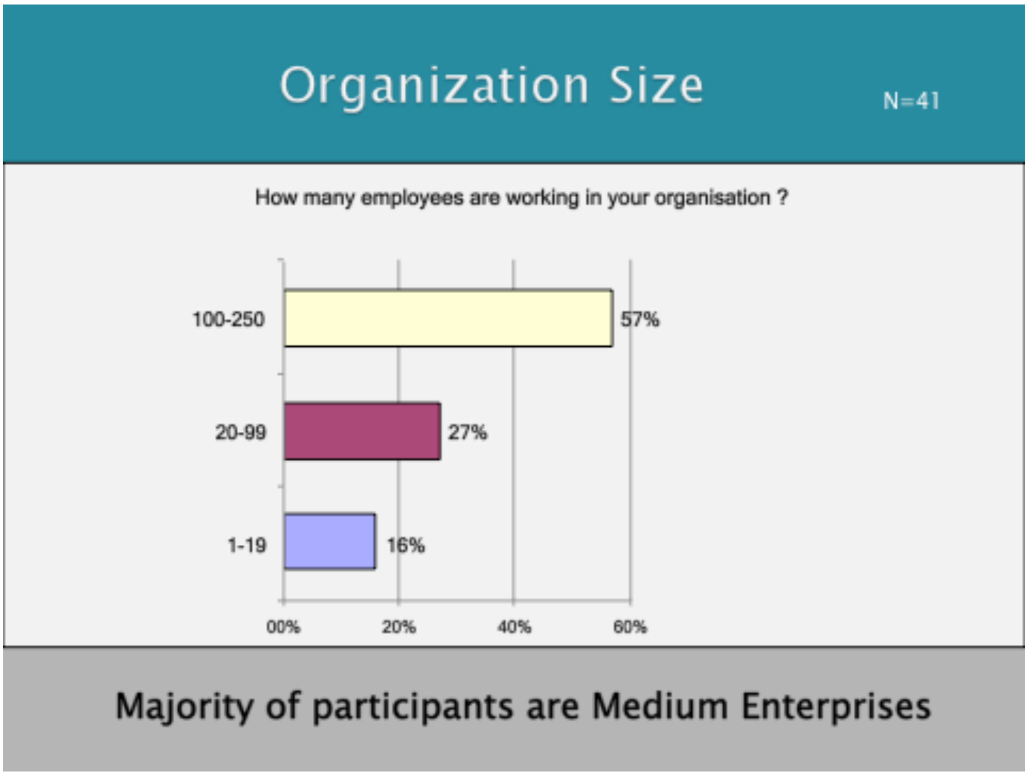
N=23

How many employees are working in your organisation ?

Majority of participants are medium enterprises

Figure 18: Organization Size of Norway MSME's

In the India MSME survey, 16.2 percent of participants were from companies with 1 to 19 employees, 27 percent of participants were from companies with 20 to 99 employees and 56.8 percent of participants were from companies with 100 to 250 employees



Organization Size

N=41

How many employees are working in your organisation ?

Majority of participants are Medium Enterprises

Figure 19: Organization Size of India MSME's

4.3 Survey Results on Norwegian MSME's

70 percent of participant's state that availability of information is the top priority security goal for Norwegian MSM

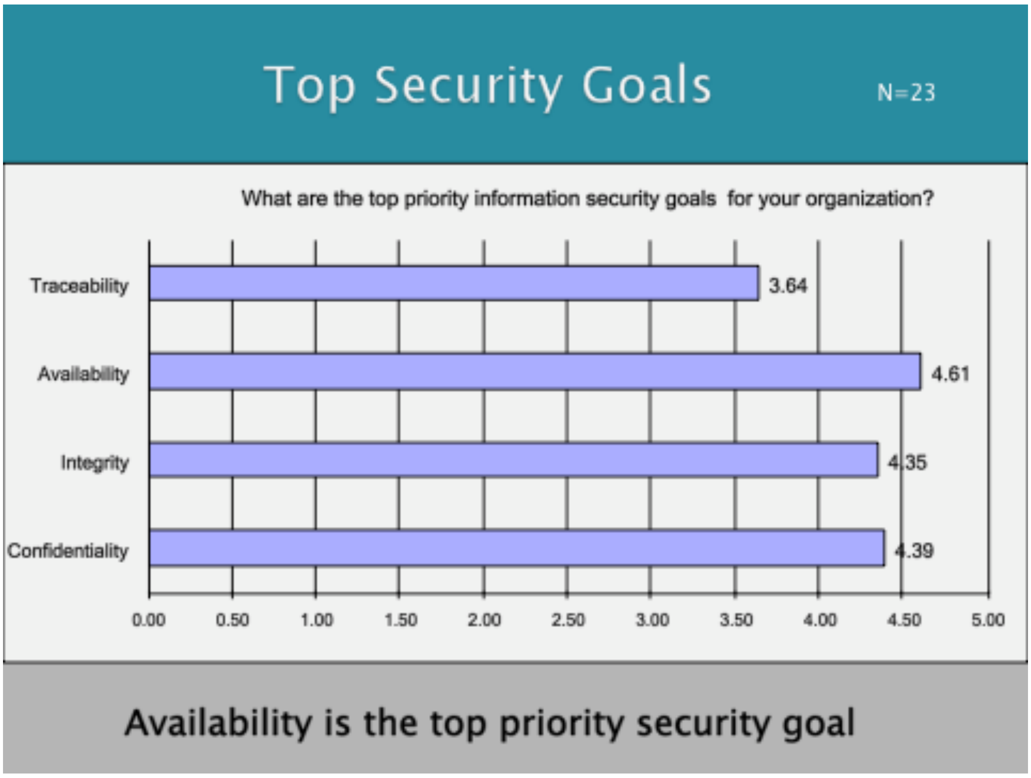
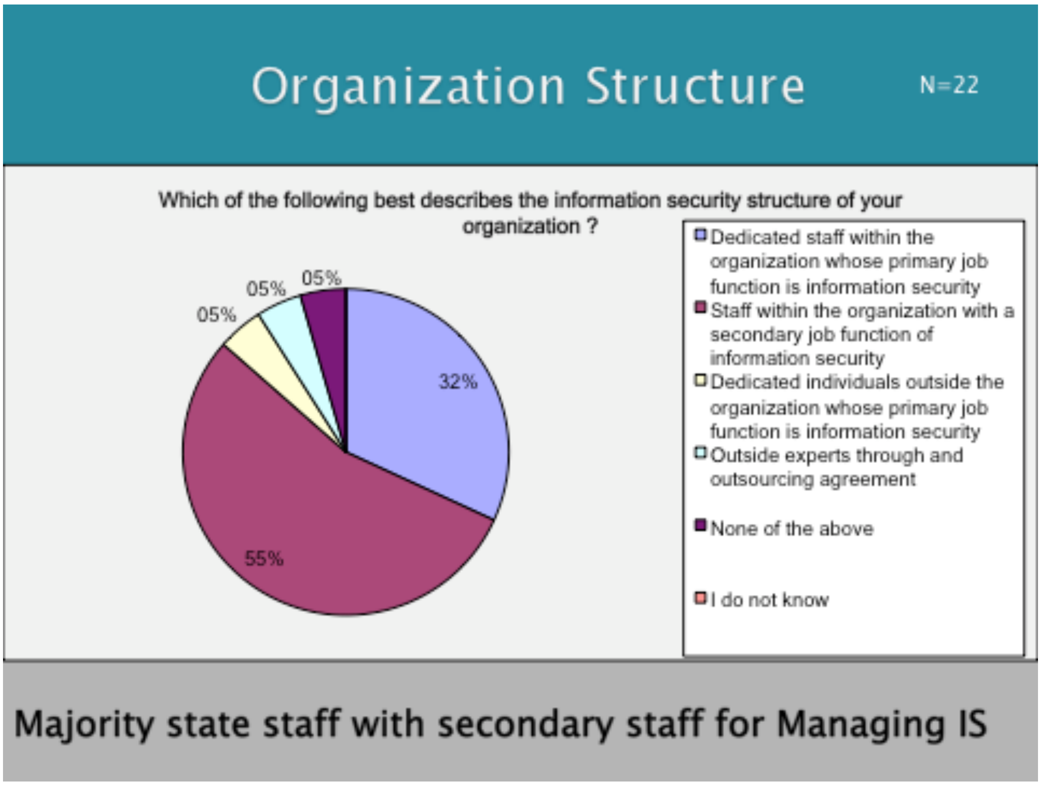


Figure 20: Top security Goals in Norwegian MSME's

The survey results indicate that the Norwegian MSME participant's state availability of information continues to be the top priority security goal for all organizations. Out of which participants from Financial Services and Government & public sector rate it as the top priority security goal. Whereas participants from IT and other sector rate confidentiality as the top priority security goal . Traceability seems to be least priority security goal for all MSME's. Participants from small and medium organizations also rate availability of information as the top priority security goal compared to micro enterprises.

55 percent of participants state that their organization have staff with secondary job function for information security



Organization Structure N=22

Which of the following best describes the information security structure of your organization ?

Majority state staff with secondary staff for Managing IS

Figure 21: Organization Structure in Norwegian MSME's

The survey results indicate that 55 percent of participants state that they have staff with secondary job function for information security, while another 32 percent state that their organization have dedicated staff . Whereas 66.7 percent of participants from financial services sector state that there organizations have dedicated staff for information security. Majority of participants from IT and Government & public sector state that their organization have staff with secondary job function for information security .75 percent of participants from medium organizations state that they have staff with secondary job function for information security.

Majority of Participants are better protecting computer and electronic data

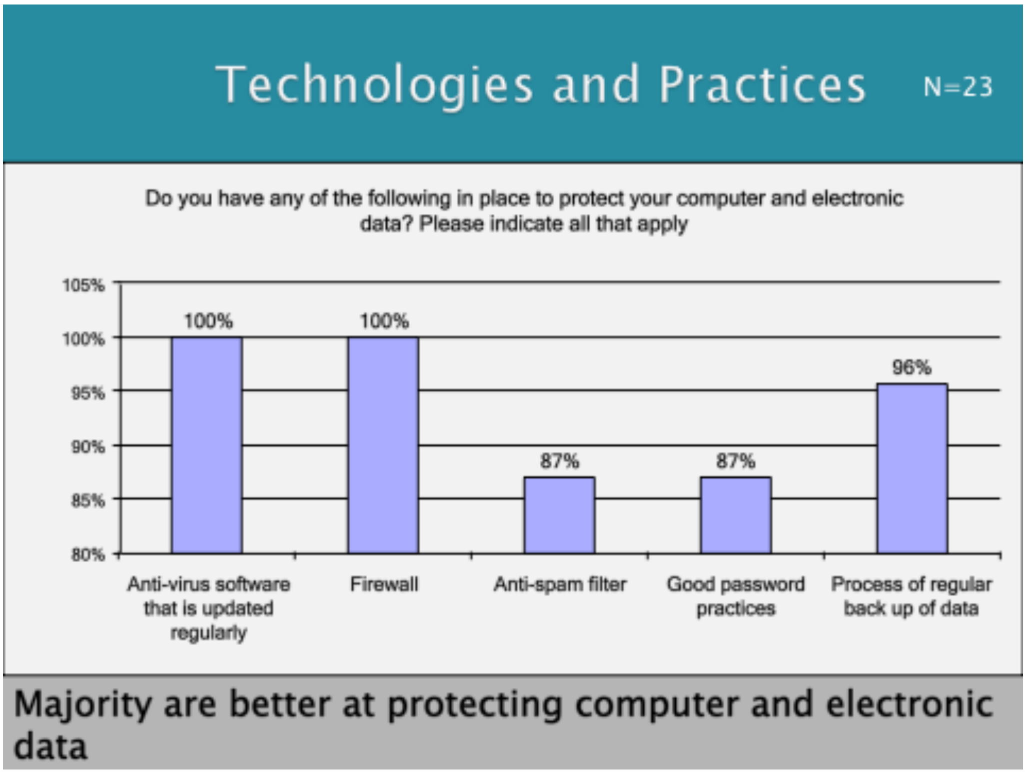
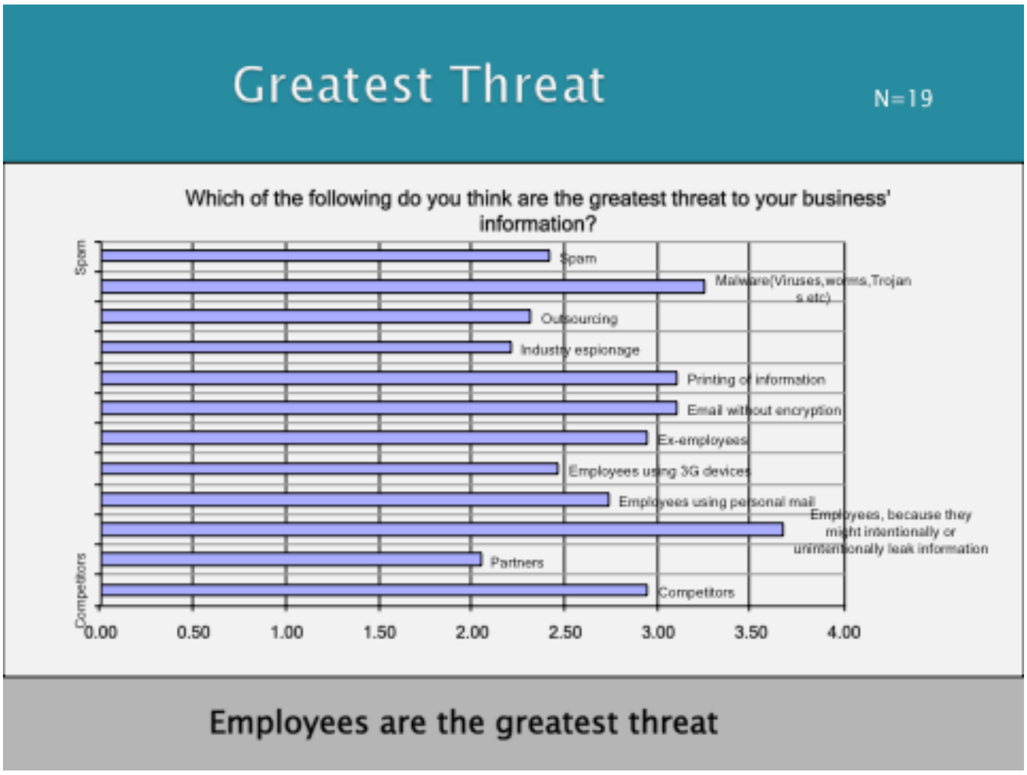


Figure 22: Technologies and Practices in Norwegian and Indian MSME's

Overall, Implementation of technologies and practices for protecting computer and electronic data continues to be a strong trend in Norwegian MSME's. Almost all participants from IT, financial services and other industry sector organizations displayed a greater interest towards adopting basic security solutions and maintaining good practices. Also participants from Government & public sector have implemented basic security solutions such as antivirus, firewalls and process of regular back up of data. Whereas only 33.3 percent of the participants from government and public sector state that they maintain security solutions like anti spam filter and maintaining good password practices. Overall , majority of Norwegian MSME have basic security solution and maintain good password practices.

Majority of participants rate that their employees are greatest threat to their business information .



Greatest Threat

N=19

Employees are the greatest threat

Figure 23: Greatest Threat in Norwegian MSME's

Majority of participants from IT, Government& public sector closely followed by other industry sector state that employees are the greatest threat to their business information as they might intentionally or unintentionally leak information. Whereas participants from financial services state competitors is their greatest threat. Majority of all participants from Micro, Small and Medium Enterprises also confirm that employees are their greatest threat as they might intentionally or unintentionally leak information.

90 percent of participants state that their organizations have security policy

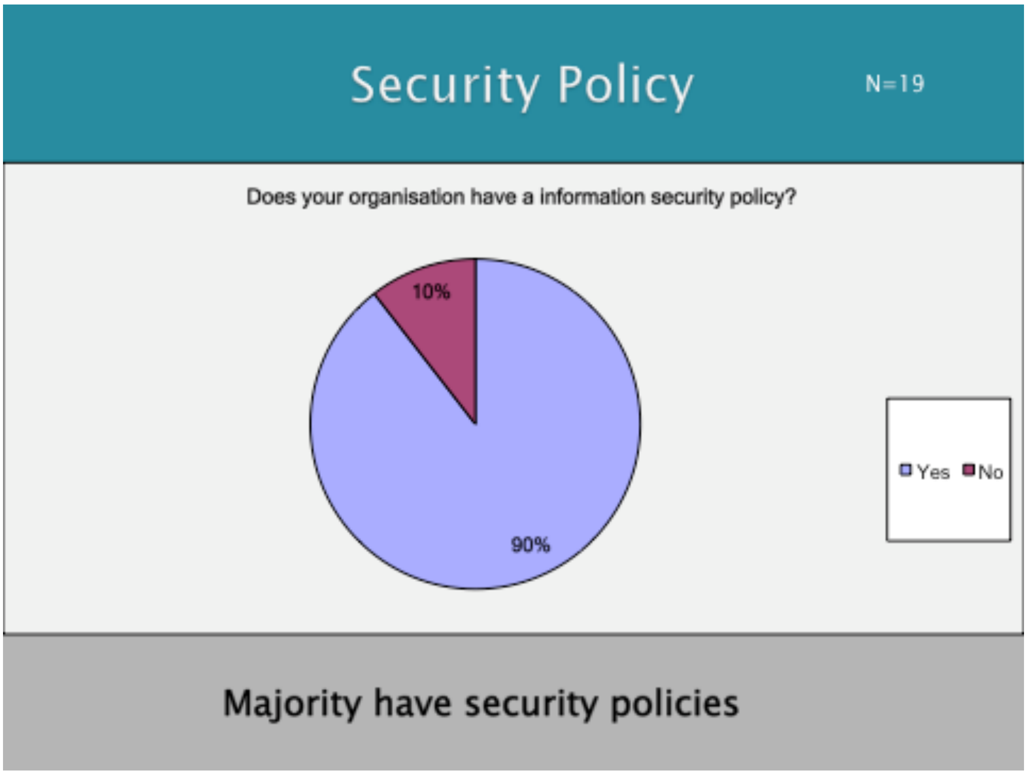


Figure 24: Security Policies in Norwegian MSME's

All participants from Government & public, financial services and other industry sector state that their organizations have security policies. Whereas only 71.4 percent of participants from IT sector state that their organizations have security policies. Majority of participants from Small and Medium organizations have security policies, whereas 33.3 percent of participants from Micro companies state that they do not have security policies

Majority of participants state that their organizations drivers for security policy are improved business practices followed by legislative regulations

.

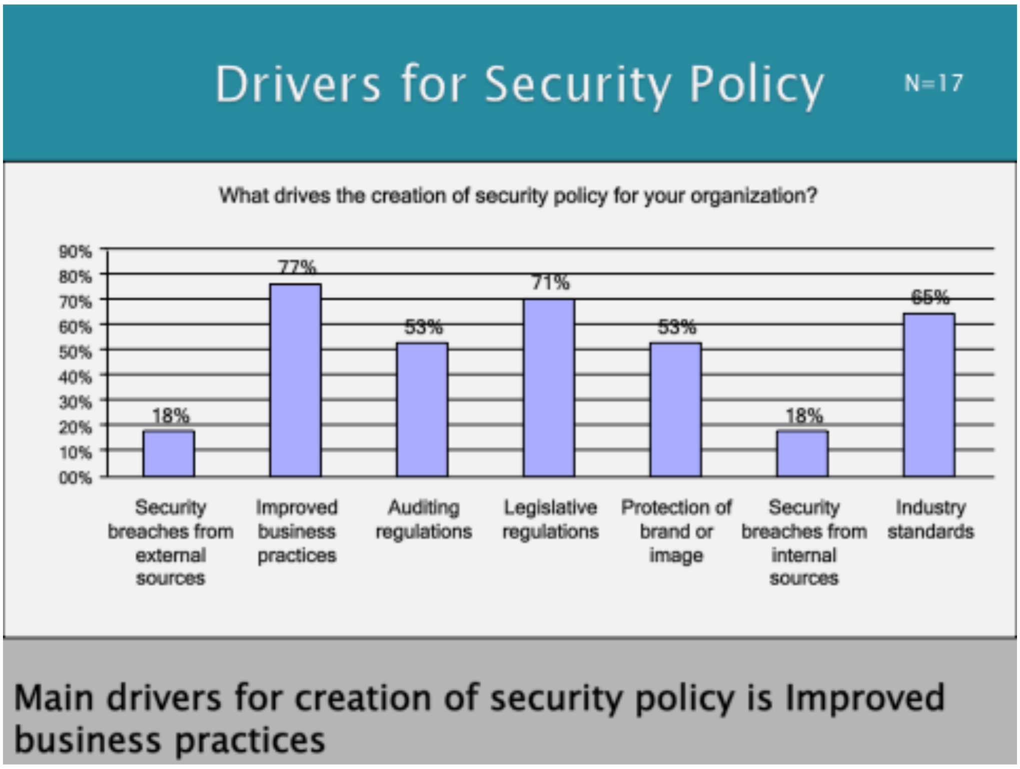
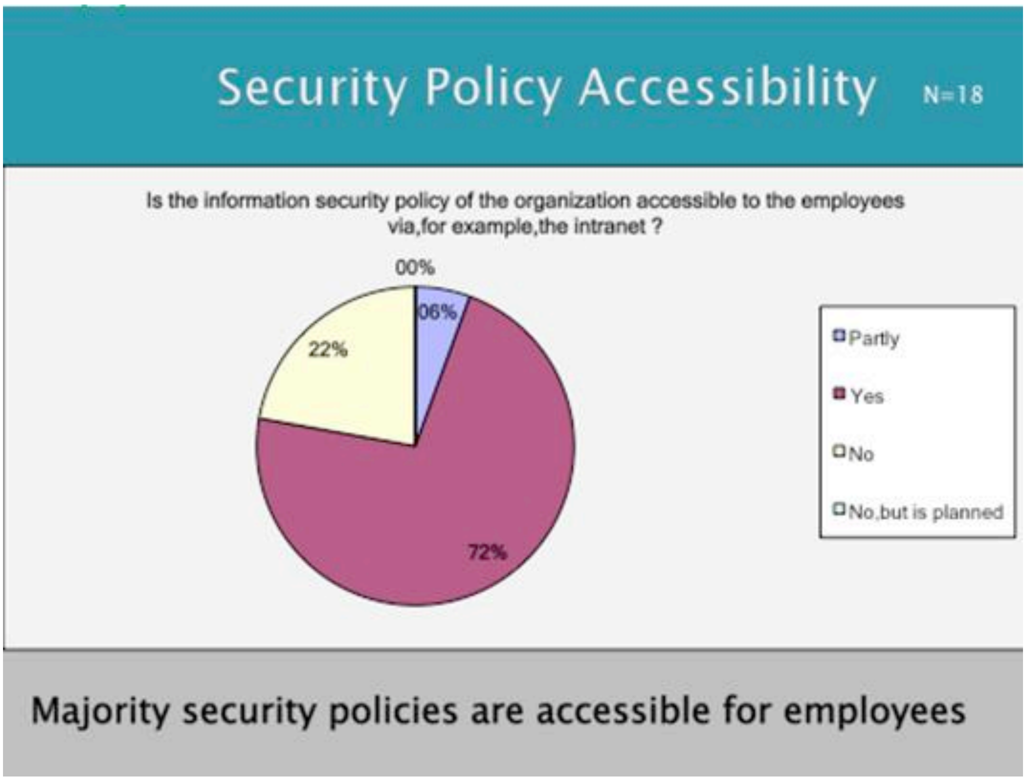


Figure 25: Drivers for Security Policies in Norwegian MSME's

All participants from financial services and Government & public sector state that their organizations main driver for security policy implementation is legislative regulations. Whereas IT, Government& public sector participants and other industry sector participants state that their organization important driver for security implementation is also improved business practices. While majority of participants from small and medium organizations state improved businesses practices. Micro organizations state legislative regulation . Majority medium enterprises state improved business practices, auditing regulations, legislatives, protection of brand or image, industry standards as they key driver creation of security policy.

72 Percent of Participants state that their organizations security policy is accessible to employees



Security Policy Accessibility N=18

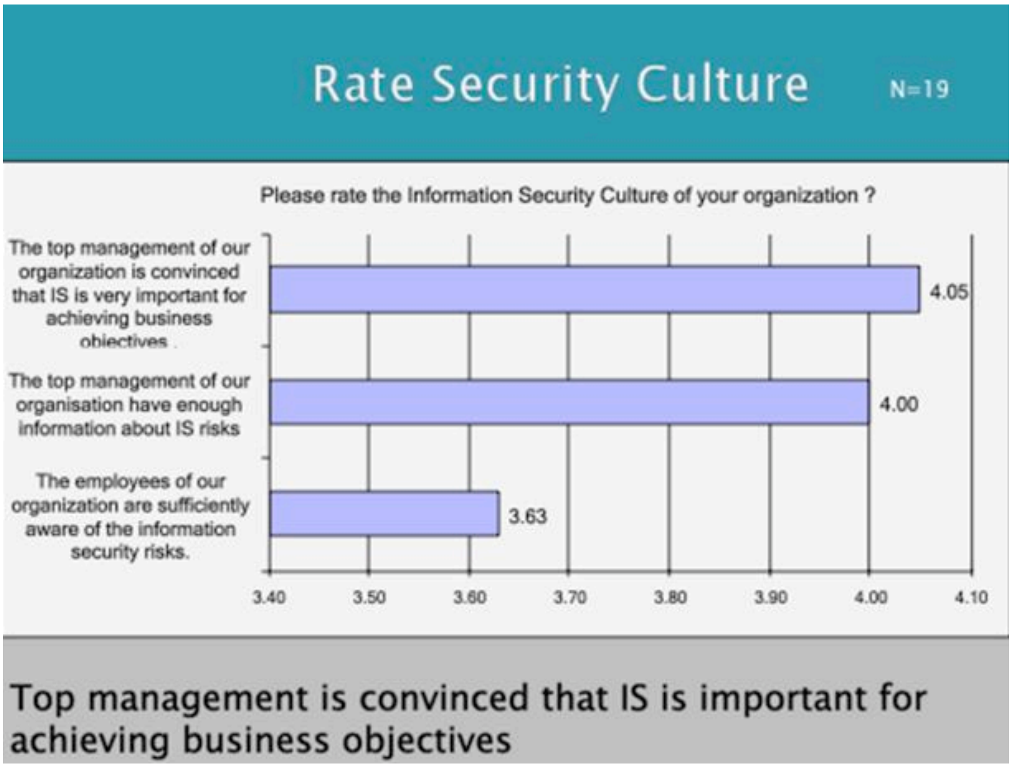
Is the information security policy of the organization accessible to the employees via,for example,the intranet ?

Majority security policies are accessible for employees

Figure 26: Security Policy Accessibility in Norwegian MSME's

Almost all participants from financial services and other industry sector state that their security policies are accessible to employees. Whereas only 50 percent from IT, 66.7 percent from Government & public sector state that they are accessible.83.3 percent of participants from small organizations state that security policies are accessible and approximately 65 percent from micro and medium state that they have access to security policies.

Majority of participants state that their organizations top management is convinced that information security is very important .



Rate Security Culture N=19

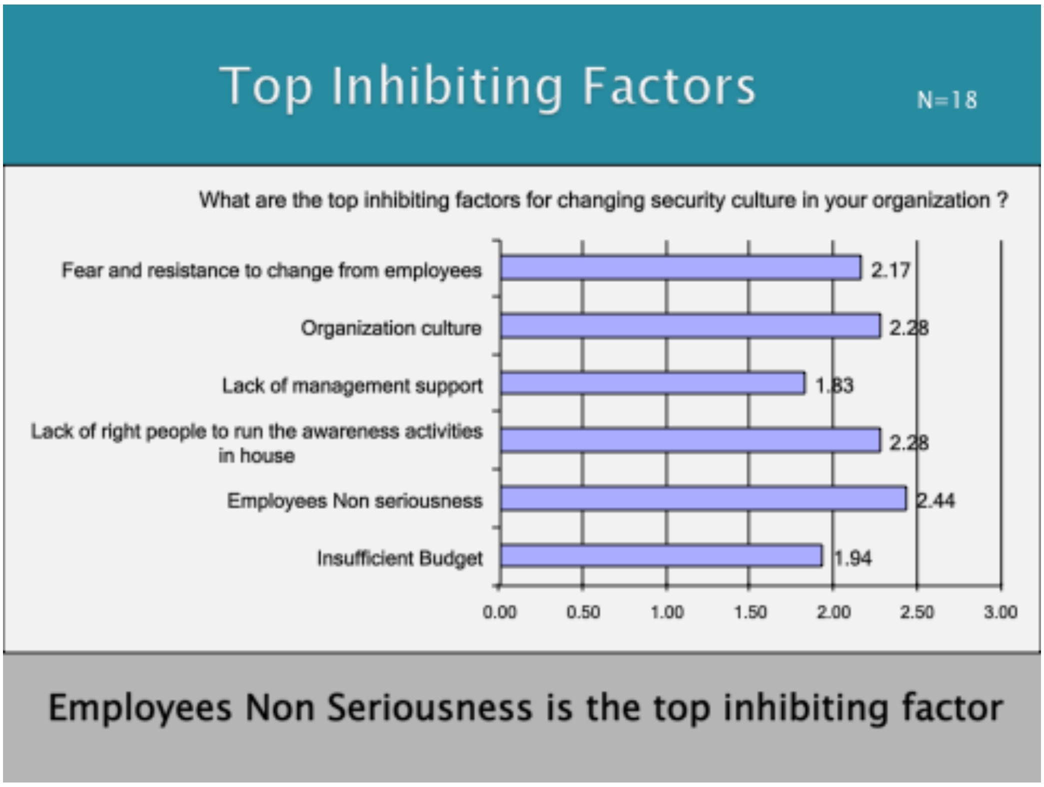
Please rate the Information Security Culture of your organization ?

Top management is convinced that IS is important for achieving business objectives

Figure 27: Rate Security Culture in Norwegian MSME's

All Participants from IT, Financial services, Government & public and other industry sector MSME's state that their organization top management is convinced that information security is very important for achieving business objectives to a very high degree. Whereas participants from Government and public sector also rate equally that employees are sufficiently aware of information security risks and convinced that information security is very important .

Majority of participants state that Employees Non Seriousness is the top inhibiting factors for changing the security culture in their organizations.



Top Inhibiting Factors N=18

What are the top inhibiting factors for changing security culture in your organization ?

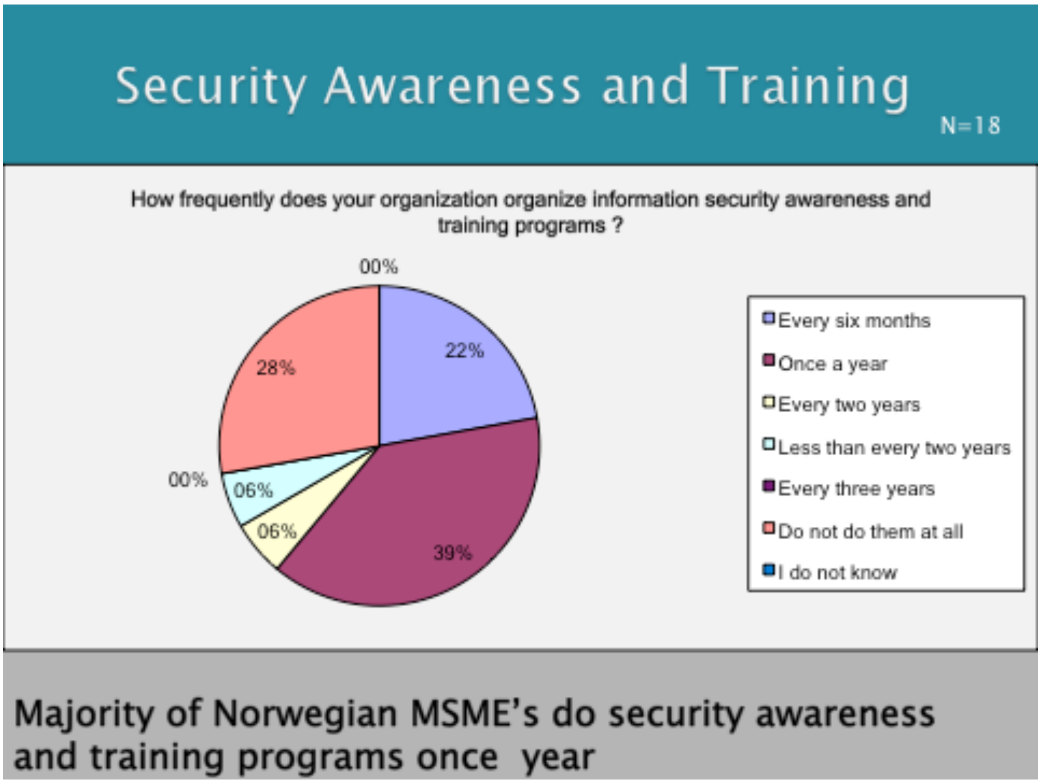
Employees Non Seriousness is the top inhibiting factor

Figure 28: Top Inhibiting Factors in Norwegian MSME's

Overall results show that different industry sector have different inhibiting factors. Participants from IT sector state that employee's non seriousness, organization culture and lack of right people to run the awareness activities are the top inhibiting factors. Whereas participants from financial services state that lack of management support, organization culture closely followed by employee's non seriousness and lack of right people to run the awareness activities are the inhibiting factors. Participants from Government & public sector state employees non seriousness, insufficient budget and lack of right people to run the awareness activities, fear & resistance to change from employees and organization culture are the top inhibiting factors .Whereas participants from other sector state that lack of right people to run the awareness activities, fear and resistance to change from employees and organization culture are top inhibiting factors for the change in security culture.

Participants from micro organizations state that fear and resistance to change from employees as their top inhibiting factor. Medium organization state lack of right people and small state employee non-seriousness are the inhibiting factors.

39 percent or majority of participants state that their organization do security awareness and training programs once a year



Security Awareness and Training

N=18

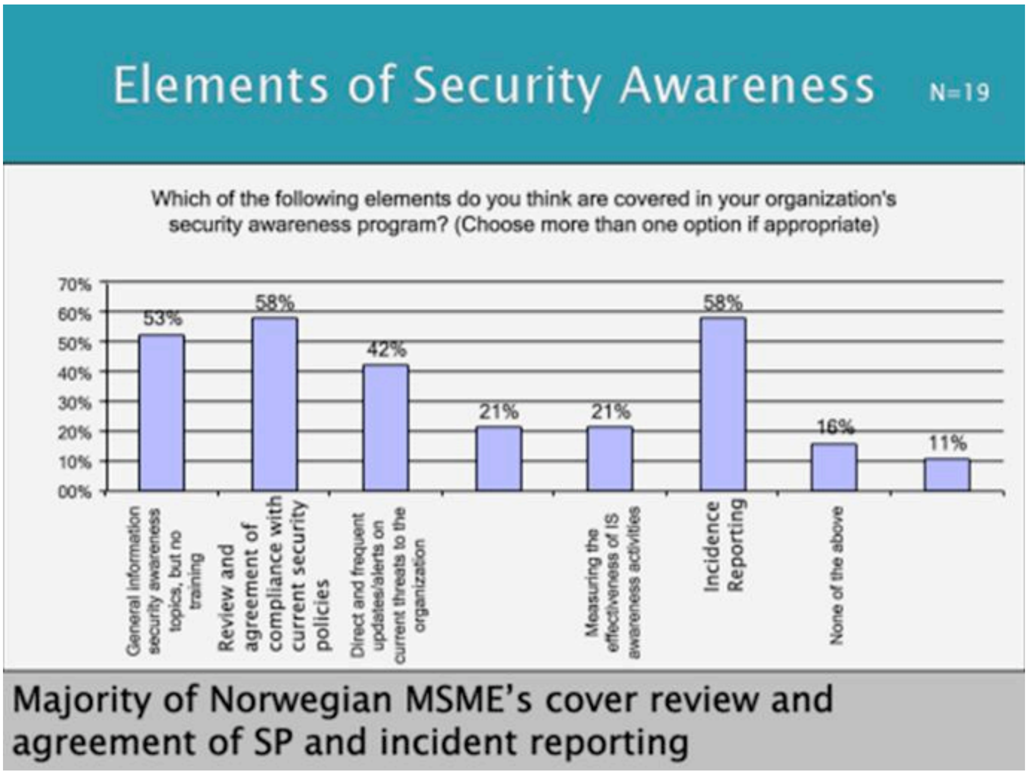
How frequently does your organization organize information security awareness and training programs ?

Majority of Norwegian MSME's do security awareness and training programs once year

Figure 29: Security Awareness and Training in Norwegian MSME's

All participants from other industry sector state that their organization does security awareness and training programs once a year. While equal numbers of participants from financial services state that their organizations do security awareness and training programs every 6 months, once a year and every two years. Majority IT participants state that they do security awareness and training programs every 6 months, once a year, less then every 2 years and other hand 67 percent participants from government & public sector state that they do not do them at all. Majority of participants from medium enterprises state that they do security awareness and training programs every 6, 12 months. Whereas small enterprises do them every 6, 12 months and less then every 2 years .

58 percent of participants state that incident reporting, review and agreement of compliance with current security policies elements are mostly covered in organization security awareness and training programs.



Elements of Security Awareness N=19

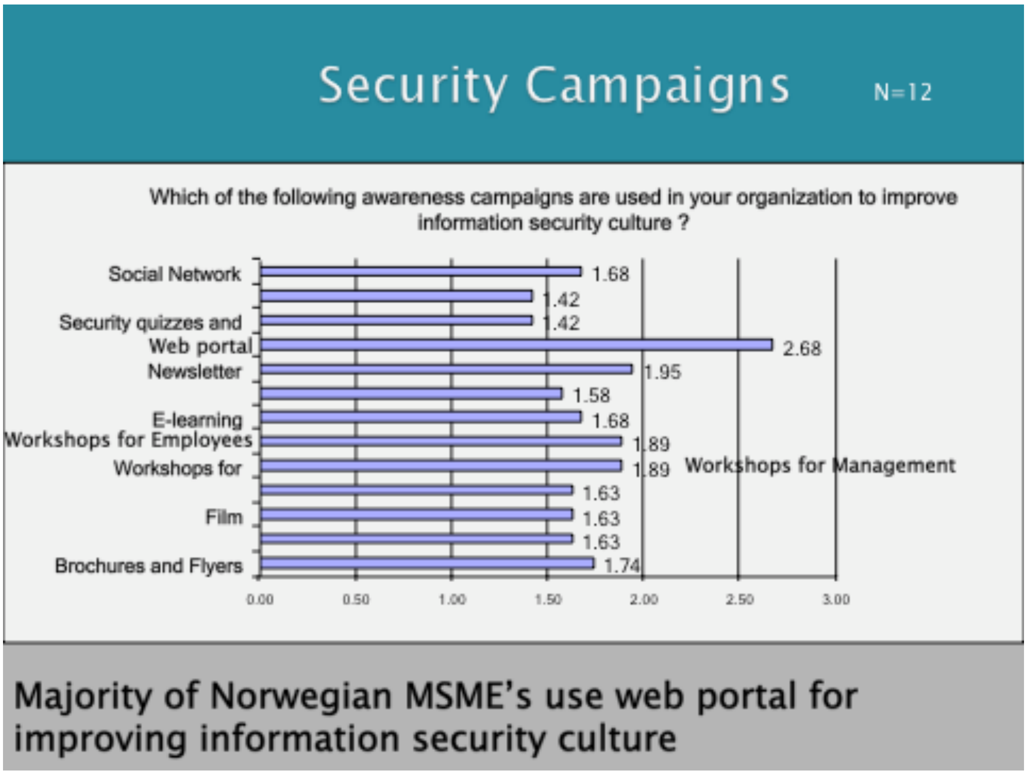
Which of the following elements do you think are covered in your organization's security awareness program? (Choose more than one option if appropriate)

Majority of Norwegian MSME's cover review and agreement of SP and incident reporting

Figure 30: Elements of Security awareness in Norwegian MSME's

Overall results show that incidence reporting and review & agreement of compliance with security policies are mainly covered in their security awareness and training programs. Financial services and other industry sector participants state review and agreement of compliance with current security policy and standards, incidence reporting the mostly covered topics. Government& public sector state general information security awareness topics and incidence reporting the mostly covered topics. Micro and Medium enterprises state review and agreement of compliance, incidence reporting as the main topics covered are security awareness and training programs.

Overall, Majority of participants state that web portal is mainly used in their organization for improving security culture



Security Campaigns N=12

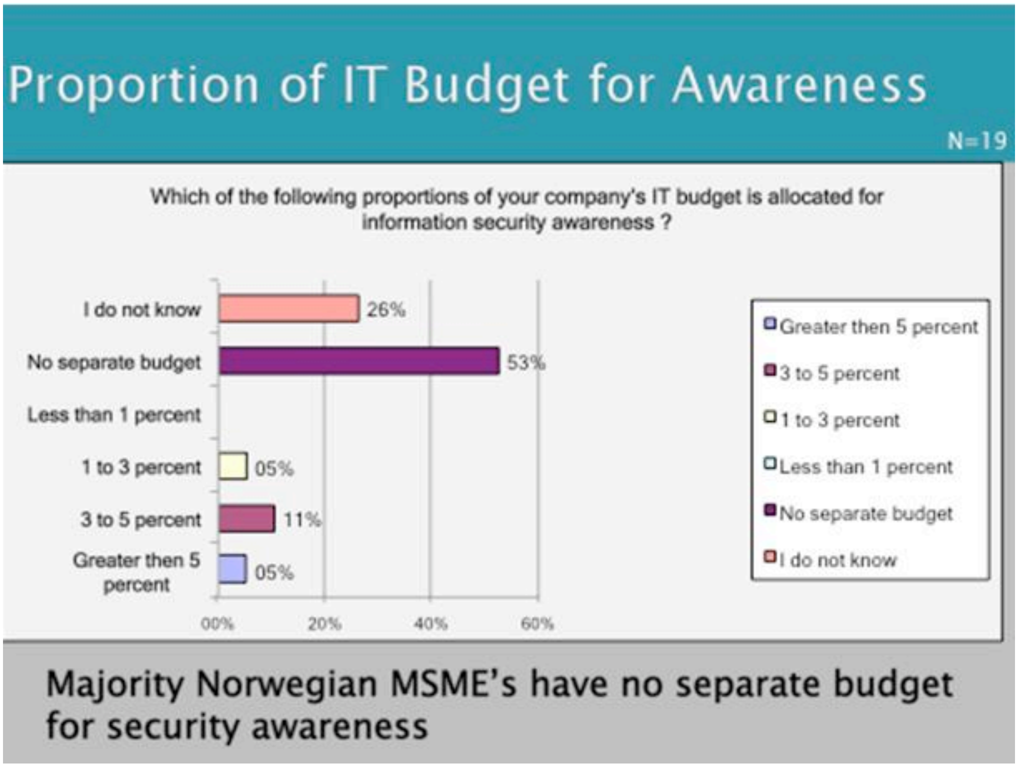
Which of the following awareness campaigns are used in your organization to improve information security culture ?

Majority of Norwegian MSME's use web portal for improving information security culture

Figure 31: Security Campaigns in Norwegian MSME's

Majority from IT, Government& public and other industry sector state that web portal is widely used in their organizations to improve information security culture. Participants from financial services state that workshops for management are also widely used. IT and other industry sector state that workshops for employees .Whereas small and medium organizations state that website are widely used in their organization for improving information security culture in their organization.

53 percent of participants state that their organizations do not have separate budget for security awareness



Proportion of IT Budget for Awareness

N=19

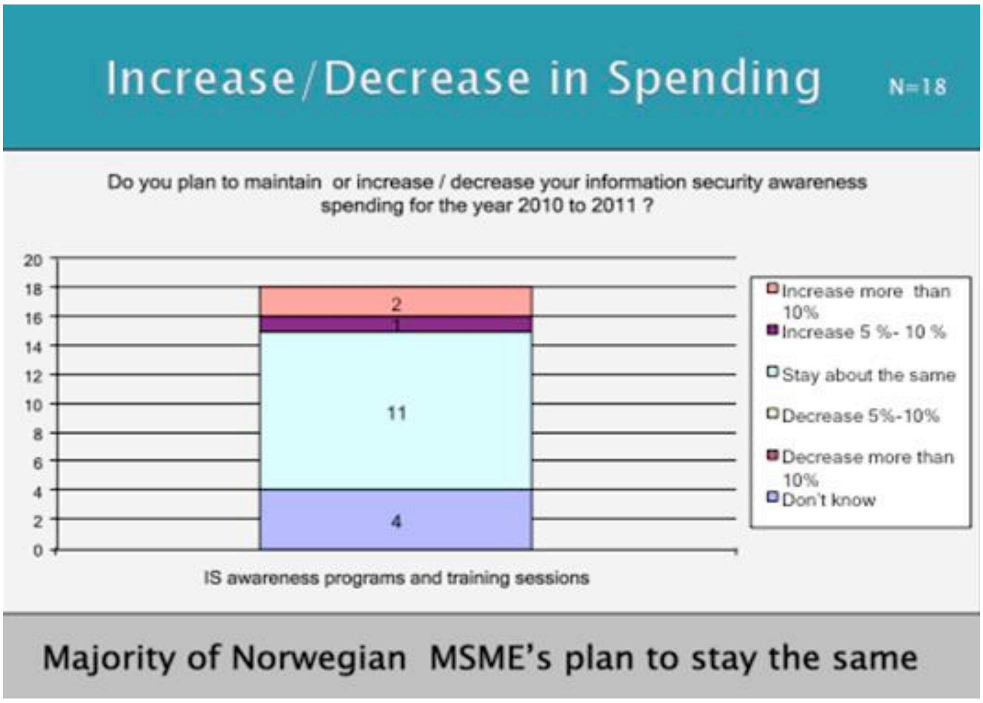
Which of the following proportions of your company's IT budget is allocated for information security awareness ?

Majority Norwegian MSME's have no separate budget for security awareness

Figure 32: Proportion of IT Budget for Awareness in Norwegian MSME's

Majority of participants from IT, Financial services, Government& public and other industry sector state that their organization do not have separate budget for security awareness.33.3 Percent of participants from financial services sector state that they spend 3 to 5 percent of IT budget for security awareness. Majority of participants from micro and medium do not have separate budget for security awareness.

61 percent of participants state that their organizations would like to spend the same on security awareness



Increase/Decrease in Spending N=18

Do you plan to maintain or increase / decrease your information security awareness spending for the year 2010 to 2011 ?

Majority of Norwegian MSME's plan to stay the same

Figure 33: Increase/Decrease in Spending in Norwegian MSME's

MSME organizations from IT, Financial services, Government & public and other industry sectors participants state that spending on security awareness and training programs to stay the same .Whereas 33.3 percent of participants from Government and Public sector state that they would like increase more than 10 percent.

Majority of participants from micro, small and medium enterprises participants state that they would like to remain the same on spending for security awareness.

4.4 Survey Results on Indian MSME's

70 percent of participant's state that confidentiality of information is the top priority security goal for Indian MSME's .

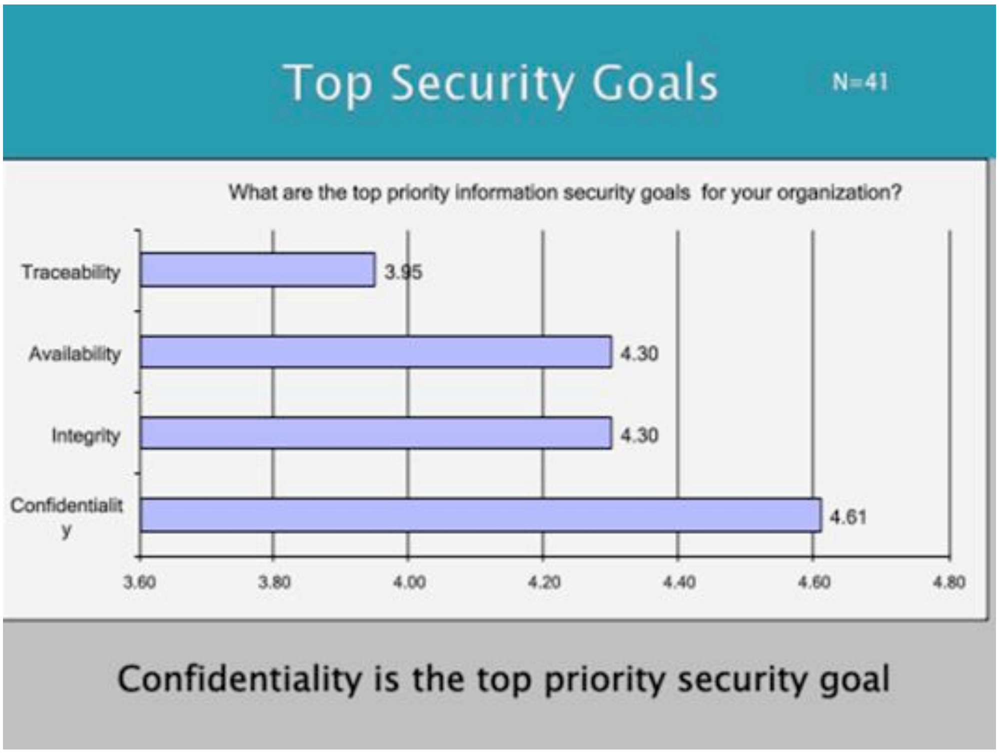
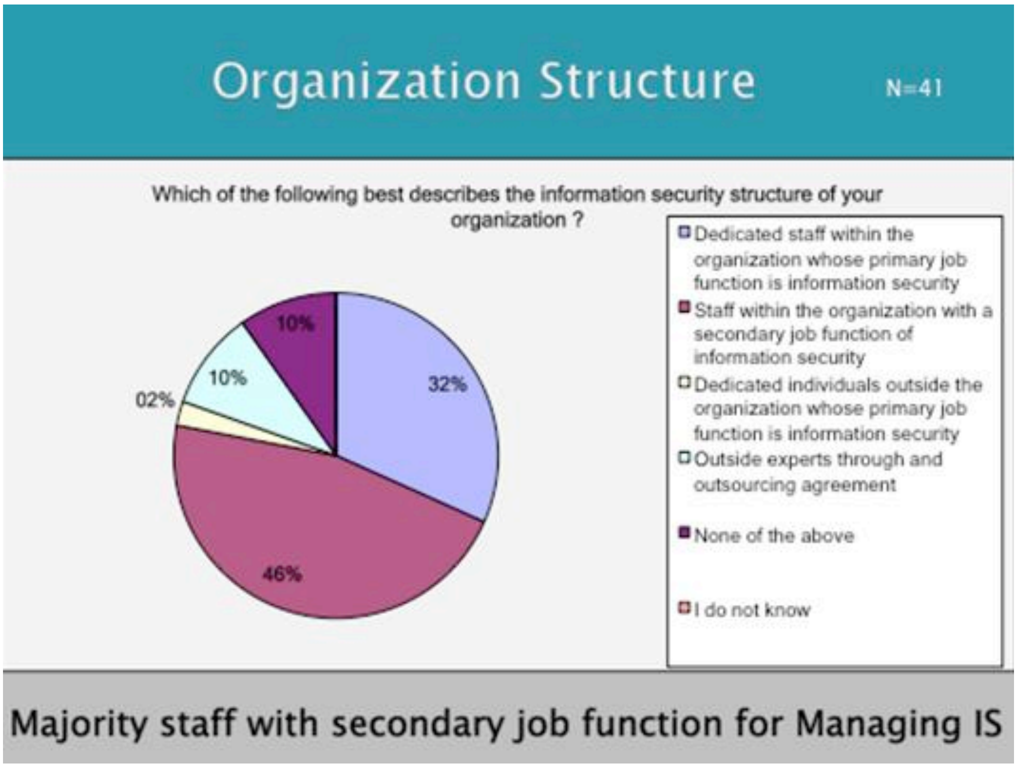


Figure 34: Top Security Goals in Indian MSME's

Majority of participants from IT, financial services and pharmaceutical state confidentiality of information continues to be the top priority security goal for all MSME organizations. Out of which ,IT, Financial services ,pharmaceutical and other sector enterprises state confidentiality as their top priority security goal, Government & public sector state availability as their top priority security goal. Availability information continues to be second priority for all the survey participants, followed by integrity. Participants of micro organizations state confidentiality & availability as their top security goal, small state confidentiality as their top security goals, whereas medium organizations state availability as their top priority security goal.

Overall, 46 percent of participants state that their organization has staff within their organization whose secondary job function is information security



Organization Structure N=41

Which of the following best describes the information security structure of your organization ?

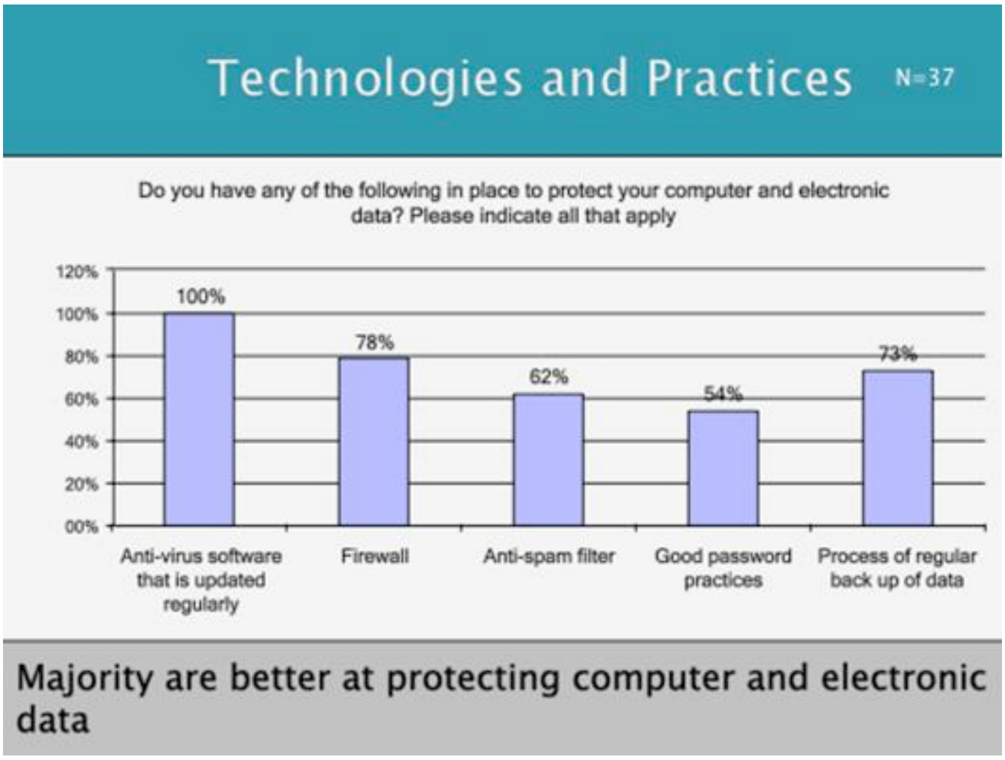
Majority staff with secondary job function for Managing IS

Figure 35: Organization Structure in Indian MSME's

Overall, 46 percent of participants state that their organizations shave staff with secondary job function and 32 percent of participants state that their organization have dedicated staff for managing information security. While 60 percent of participants from financial services sector state that they have dedicated staff and 20 percent state that they have staff with secondary job function. IT and other industry sector state that their organization has approximately 64.7 percent staff with secondary job function. 16.7 percent participants from pharmaceuticals state that their organization have dedicated staff with secondary job function for information security. Whereas government & public sector participants state that they have dedicated, on dedicated and outside experts. Other industry sector participants state that 62.5 percent of them have staff with secondary job function for information security.

More than 66 percent of participants from Micro and Small state that they have staff with secondary job function for information security. Whereas participants from medium organizations state that they have 47.6 percent dedicated staff and 33.3 percent as secondary staff for information security.

Majority of all participants have implemented basic information security solution for protecting computer and electronic data.



Technologies and Practices N=37

Do you have any of the following in place to protect your computer and electronic data? Please indicate all that apply

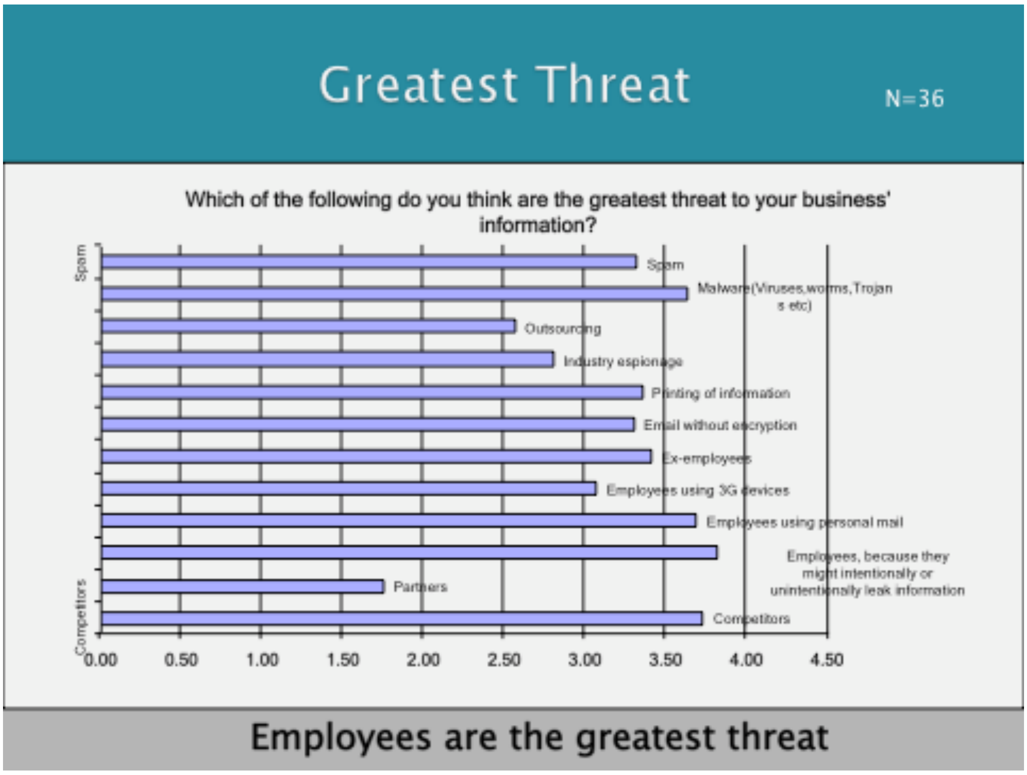
Majority are better at protecting computer and electronic data

Figure 36: Technologies and Practices in Indian MSME's

Overall, 78 percent state that their organizations have firewalls, out of which all participants from Government & public sector have implemented them. All participants from IT sector are maintaining antivirus, firewall and back up of data and few are also not maintaining anti spam filter and good password practices. Participants from financial services are maintaining antivirus, but there is also around 40 percent not maintaining firewalls, back up and anti spam filter. Participants from pharmaceutical are maintaining antivirus, but few do not have firewall and back up of data, with 50 percent do not even maintain spam filter and good password practices. Government & public sector maintain antivirus, but majority are not having back up and maintain good password practices. Other industry sector participant state that all maintain antivirus, but more than 40 percent do not even maintain anti spam filters and good password practices.

The results also show that all micro enterprises have antivirus, firewall, regular back up of data and more than 65 percent do not have anti spam filter. More than 80 percent small enterprises maintain antivirus, firewall, regular back up of data, but majority small enterprises do not even maintain good password practices. All in medium companies maintain antivirus, but there is quite few enterprises who do not maintaining firewalls, anti spam filters, regular back up and maintain good password practices.

Majority of participants rate that their employees are greatest threat to their business information.



Greatest Threat

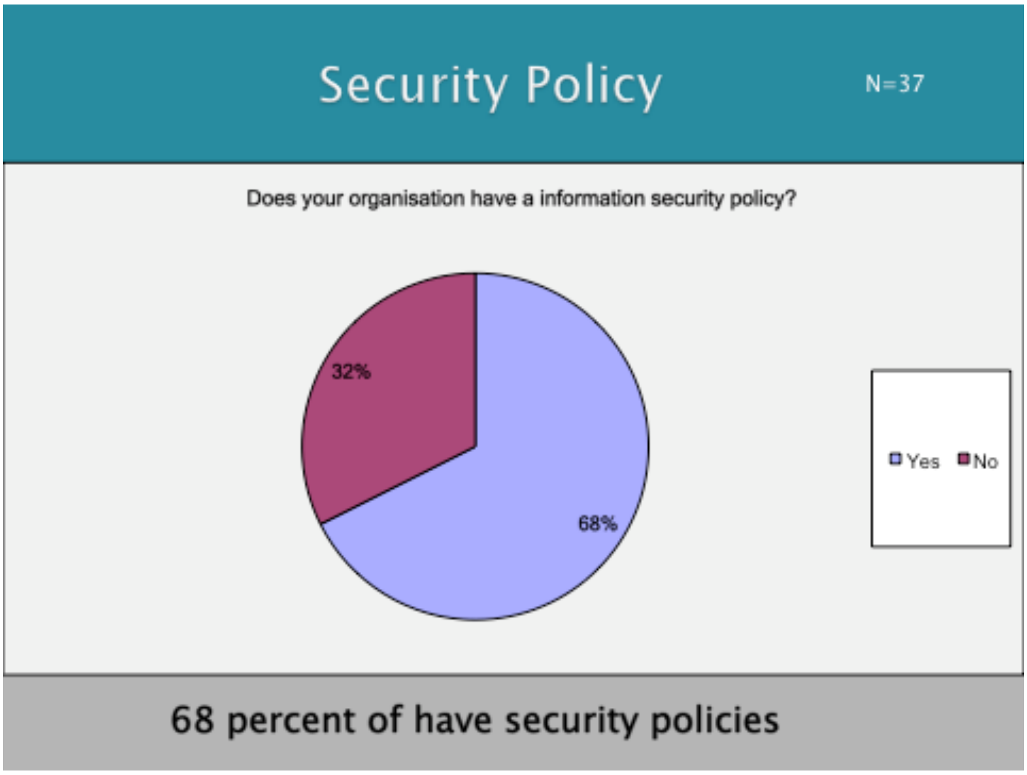
N=36

Employees are the greatest threat

Figure 37: Greatest Threat in Indian MSME's

Overall majority of MSME participants state that employees are the greatest threat to their business information as they might intentionally or unintentionally leak business information; whereas results show that different industry sectors state that they have different priorities for greatest threat. IT participants state employees, financial services state ex-employees, government& public sector state employees using personal email, malware, spam. Pharmaceutical enterprises state competitors, whereas other enterprises state malware as their greatest threat. Micro and small enterprises state competitors as their great threat. While medium enterprises state that malware and employees using personal email as their greatest threat.

68 percent of participants state that their organizations have security policy



Security Policy

N=37

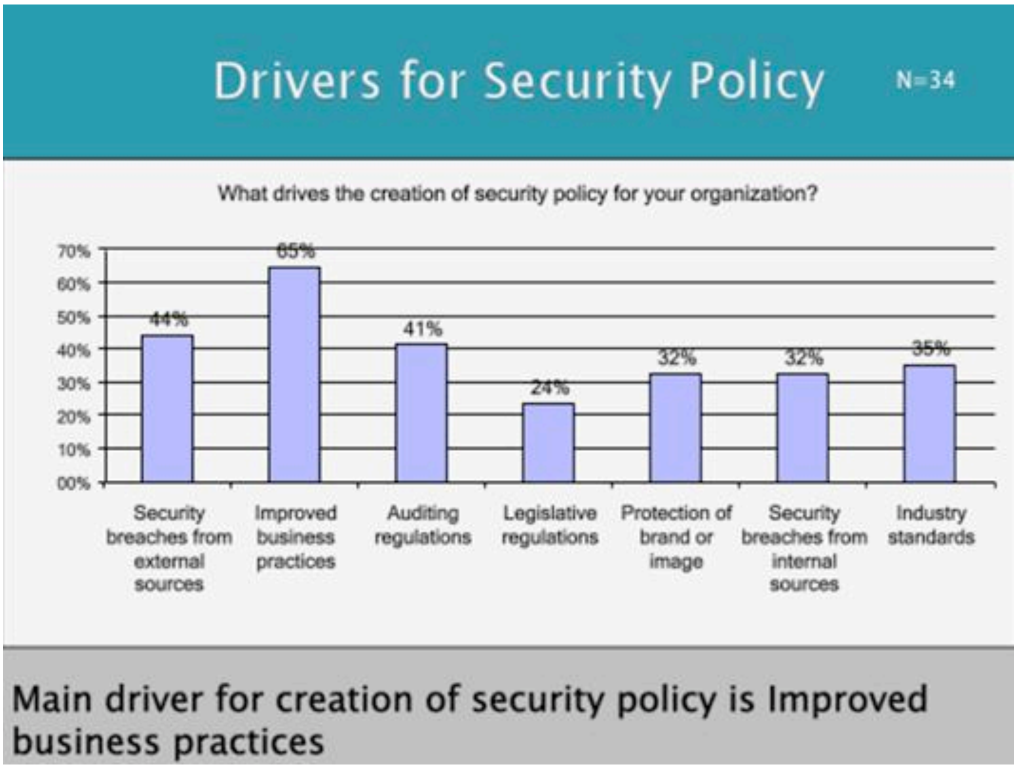
Does your organisation have a information security policy?

68 percent of have security policies

Figure 38: Security Policy in Indian MSME's

Majority of participants from IT, financial services, Government & public and other industry sector participants state that their organizations have security policies. 60 percent of participants from pharmaceuticals state that their organizations do not have securities policies. More than 67 percent of participants from small and medium organizations state that their organization has security policies. But only 50 percent of participants in micro state that they have security policies.

65 percent or Majority of participants state that their organizations drivers for security policy is improved business practices.



Drivers for Security Policy N=34

What drives the creation of security policy for your organization?

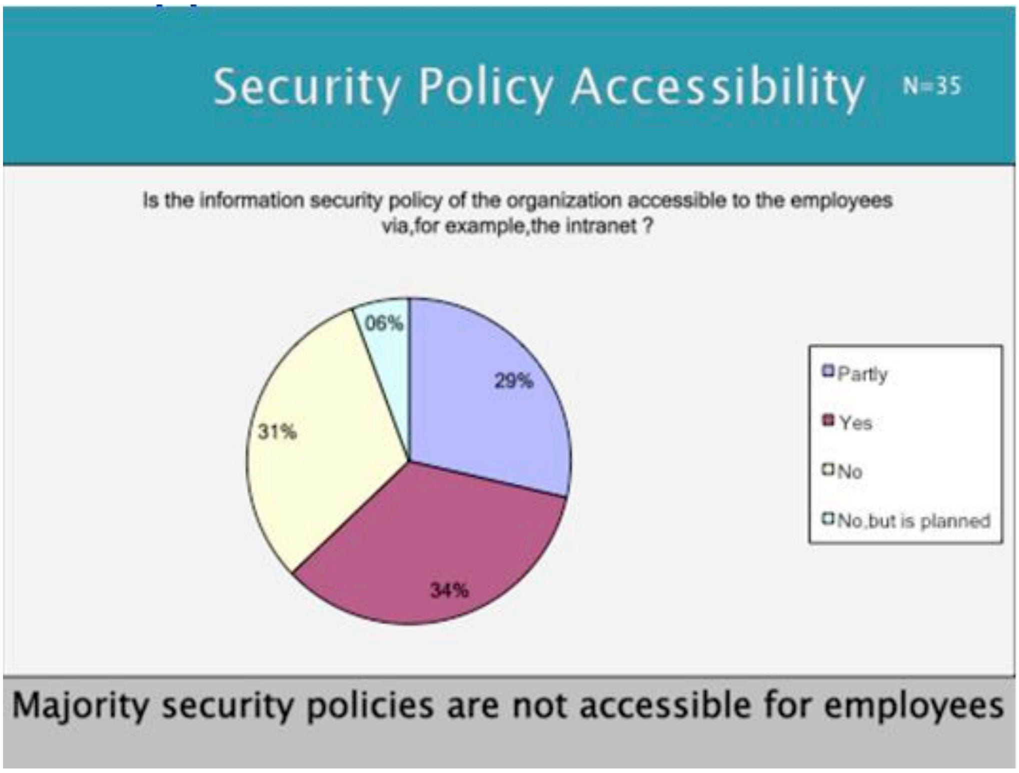
Main driver for creation of security policy is Improved business practices

Figure 39: Drivers for Security Policy in Indian MSME's

Majority of participants from financial services, IT, and other industry sector state that their organizations main driver for security policy implementation is improved business practices. 44.1 percent of participants from IT, financial services, Government& public and pharmaceutical state that their organization driver for implementation of security policy is also security breaches from external sources.41.2 percent of participants from financial services, pharmaceuticals, Government& public sector state that auditing regulations is also their important driver for security policy. The results show that apart from financial services, IT, government& public, pharmaceuticals and other industry sector do not state legislative regulations as their main driver for security policy implementation.

All participants from micro organizations state improved business practices as their driver ,Whereas majority of participants from small and medium organizations state improved business practices as an it as an important driver.

Overall, 34 percent of Participants state that their organizations security policy is accessible to employees



Security Policy Accessibility N=35

Is the information security policy of the organization accessible to the employees via,for example,the intranet ?

Majority security policies are not accessible for employees

Figure 40: Security Policy accessibility in Indian MSME's

Overall, results show that 34.3 percent of participants from IT, financial services , pharmaceutical , Government & public sector and others industry sector state that their security policies are accessible. Whereas 43.8 percent from IT, 40 percent of financial services, 50 percent in government & public sector, 20 percent in pharmaceutical, 62.5 percent in other sector state that their security policy are accessible.

Only 25 percent in micro, 33.3 in small and 35 percent from medium state that their security policy are accessible for employees.

Majority of participants rate that their organizations top management is convinced that information security is very important.

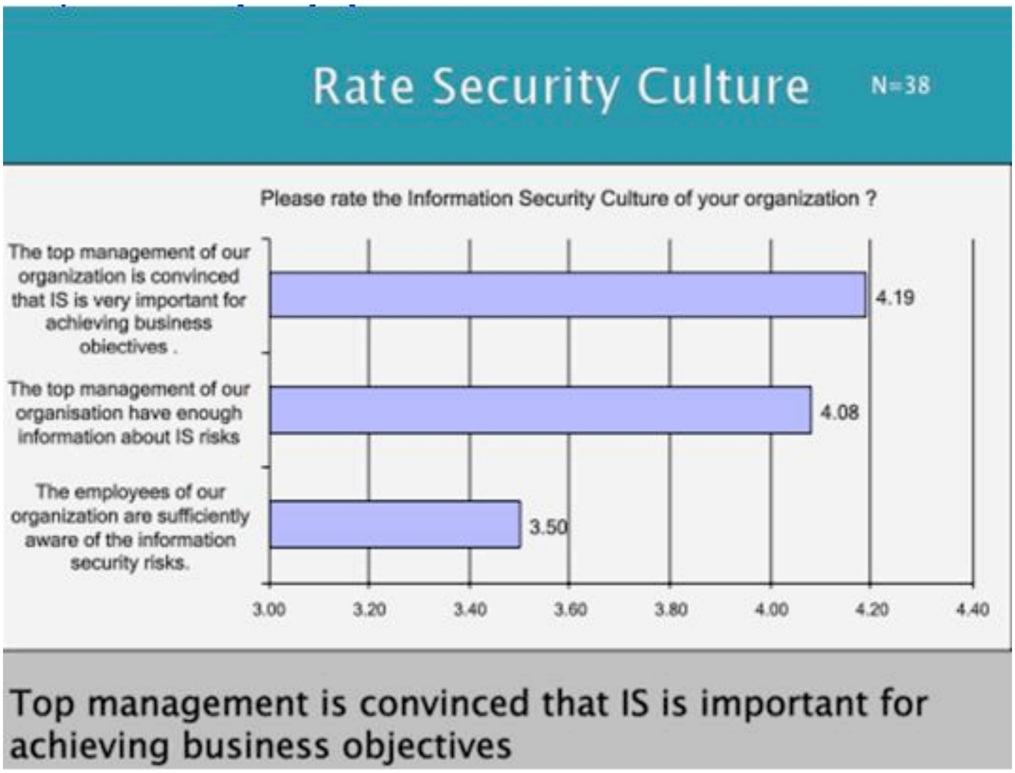


Figure 41: Rate security culture in Indian MSME's

All Participants from IT, financial services, Government & public, pharmaceutical and other industry sector states that their organization top management is convinced that information security is very important for achieving business objectives to a very high degree.

All the micro, small and medium enterprises state their top management is convinced that information security is very important for achieving business objectives to a very high degree.

Majority of participants state that Employees Non Seriousness ,followed by lack of right people to run the awareness activities in house are top inhibiting factors for changing the security culture

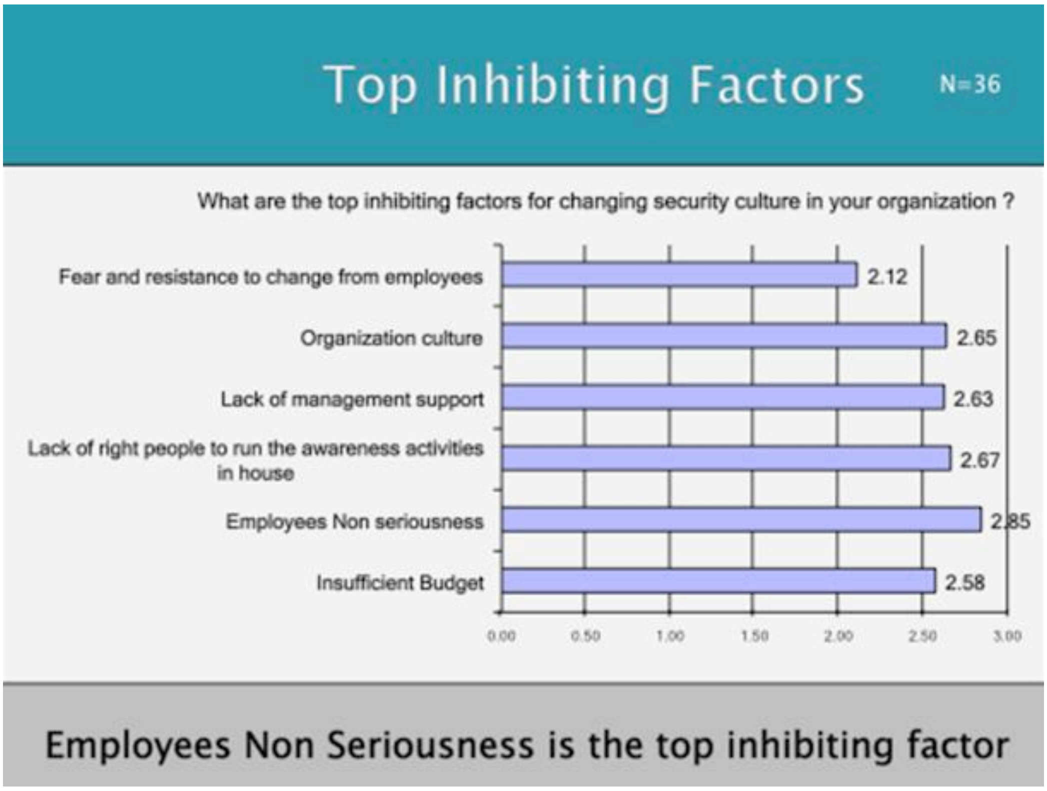
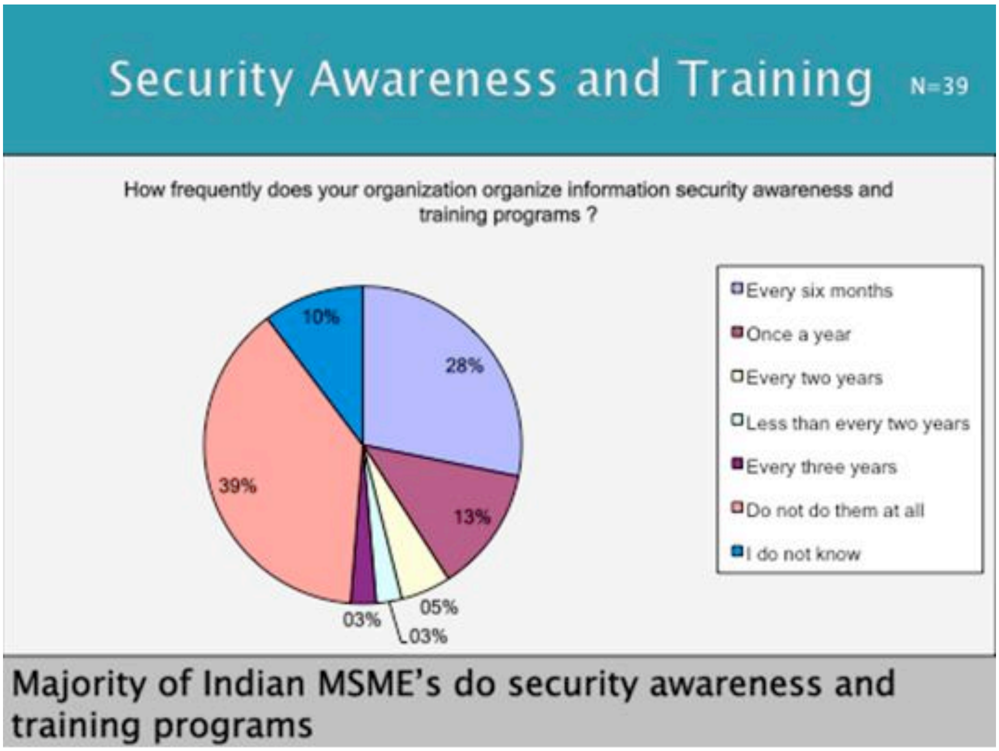


Figure 42: Top Inhibiting Factors in Indian MSME's

All participants from different industry sector have different inhibiting factors. Participants from financial services and other industry sector state that employees non seriousness to be the top inhibiting factors. Participants from IT, Pharmaceutical and other industry sector state that lack of right people to run the awareness activities in house is their top inhibiting factor. Whereas participants in Micro organization state that insufficient budget and lack of right people to run the activities be their top inhibitors. Small and Medium organizations state employee non seriousness as their top inhibiting factor.

39 percent or majority of participants state that their organization do not do security and awareness programs at all.



Security Awareness and Training N=39

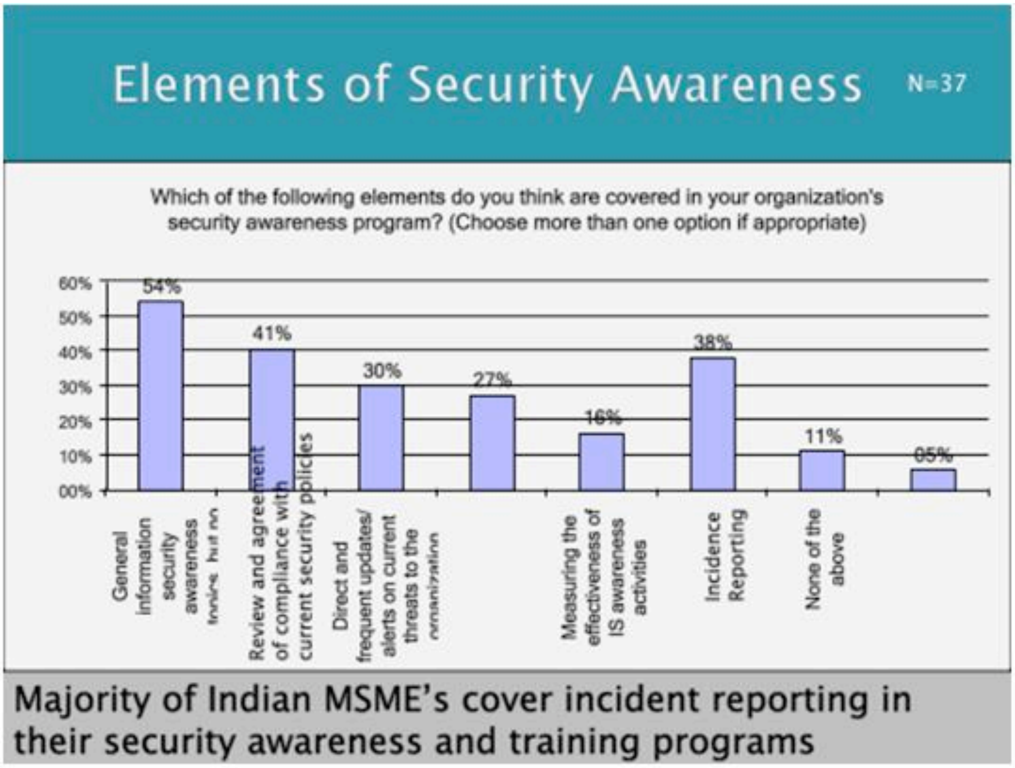
How frequently does your organization organize information security awareness and training programs ?

Majority of Indian MSME's do security awareness and training programs

Figure 43: Security awareness and Training in Indian MSME's

83.5 percent of participants from pharmaceuticals state that their organizations do not do security awareness and training programs at all. While majority of participants from IT state that their organizations do security awareness and training programs every 6, 12 months and every 2 years. Whereas 60 percent participants from financial services state that they do security awareness and training programs every 6 months and 3 years .Whereas majority micro enterprises do not do them at all, only 33.3 percent state that they do it less then every 2 years. Small and medium organization participants do security awareness and training programs between 6 months and 2 years.

54 percent or Majority of participants state that General information security awareness topic elements are mostly covered in their organization security awareness and training programs



Elements of Security Awareness N=37

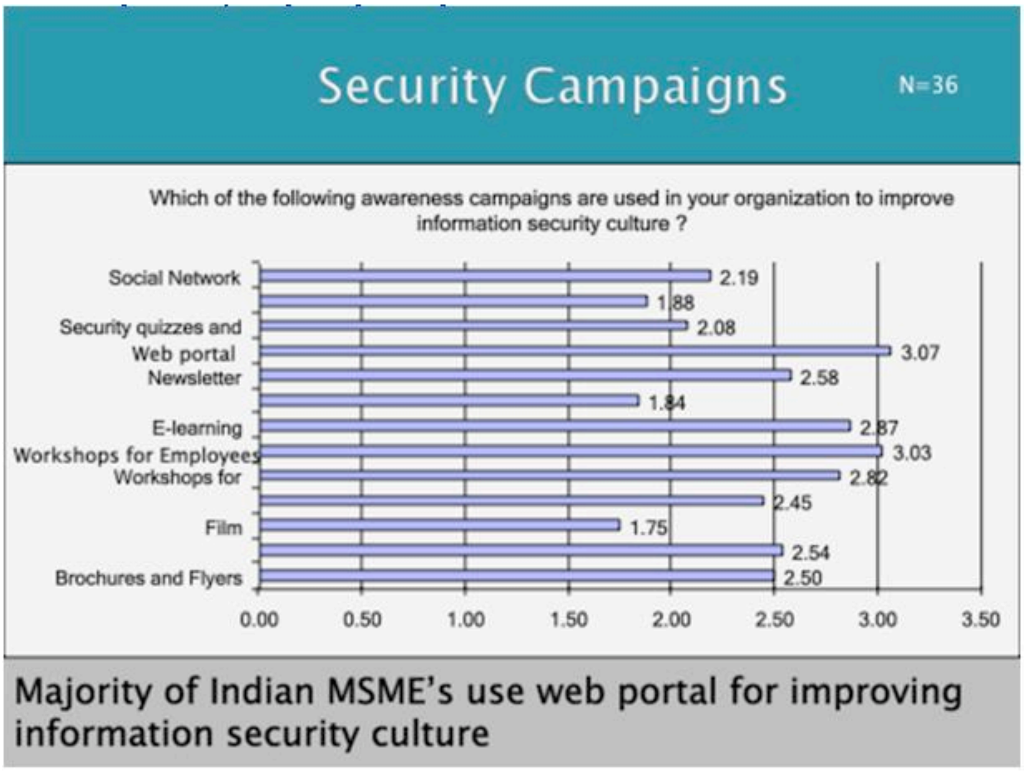
Which of the following elements do you think are covered in your organization's security awareness program? (Choose more than one option if appropriate)

Majority of Indian MSME's cover incident reporting in their security awareness and training programs

Figure 44: Elements of Security Awareness in Indian MSME's

Majority of participants from IT, financial services, pharmaceuticals , Government & public sector and other industry sector state that general information security awareness is mainly covered in their security awareness and training programs. Overall 40.5 percent of participants from IT, financial services, Government & public sector and other industry sector state that review & agreement of compliance with current security policies and standards to be the second element mostly covered. Whereas participants from IT, financial services, Government& public sector and other industry sector also state that their organization mostly covered element for security awareness is incidence reporting. 80 percent of participants from Micro organizations state general information security awareness topics as their elements, whereas small and medium organizations state general information security awareness topics, review and agreement of compliance with current security policies and incidence reporting the most used elements.

Overall, Majority of participants state that web portal, workshops for employees and e learning are used for improving security culture


Security Campaigns N=36

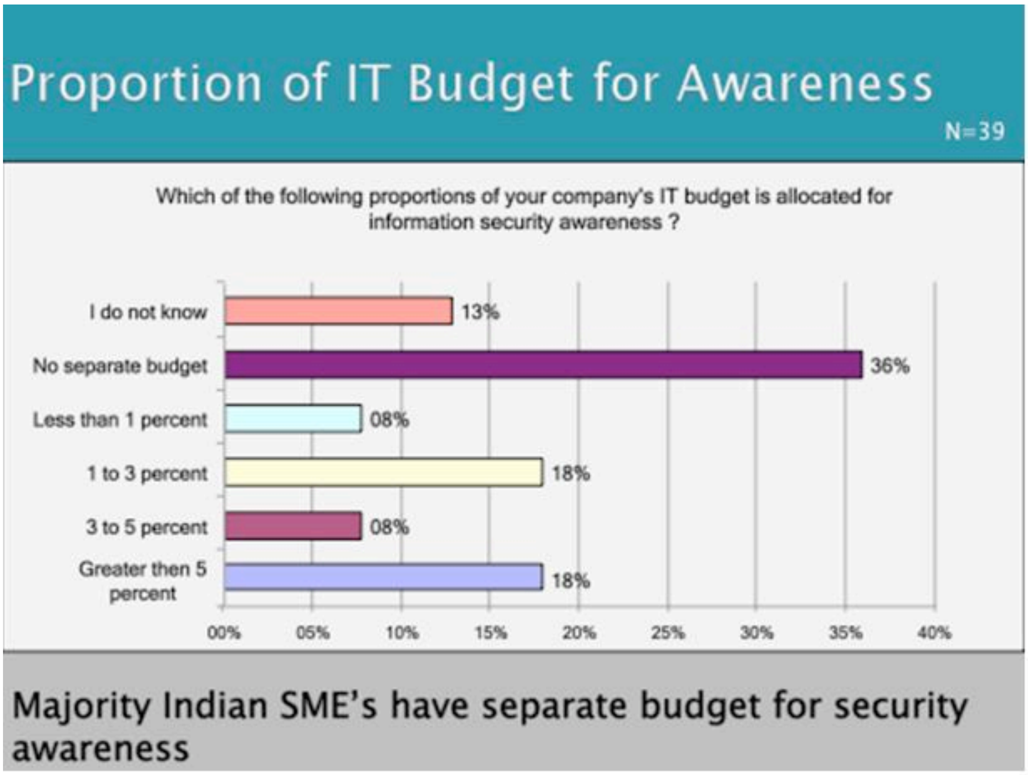
Which of the following awareness campaigns are used in your organization to improve information security culture ?

Majority of Indian MSME's use web portal for improving information security culture

Figure 45: Security Campaigns in Indian MSME's

Majority of participants from IT, financial service, Government& public and other industry sector state that web portal is widely used in their organizations to improve information security culture. Participants from IT and Government & public sector and other industry sector state that workshops for employees is widely used .Whereas participants from financial services , Government & public sector state that e learning is widely used in their organizations. Participants from medium organizations state web portal, workshops for all employees are used. Whereas micro and small state articles in news papers and workshops for all employees as their most used security campaigns.

51 percent or Majority of Participants state that their organizations do not have a separate budget



Proportion of IT Budget for Awareness

N=39

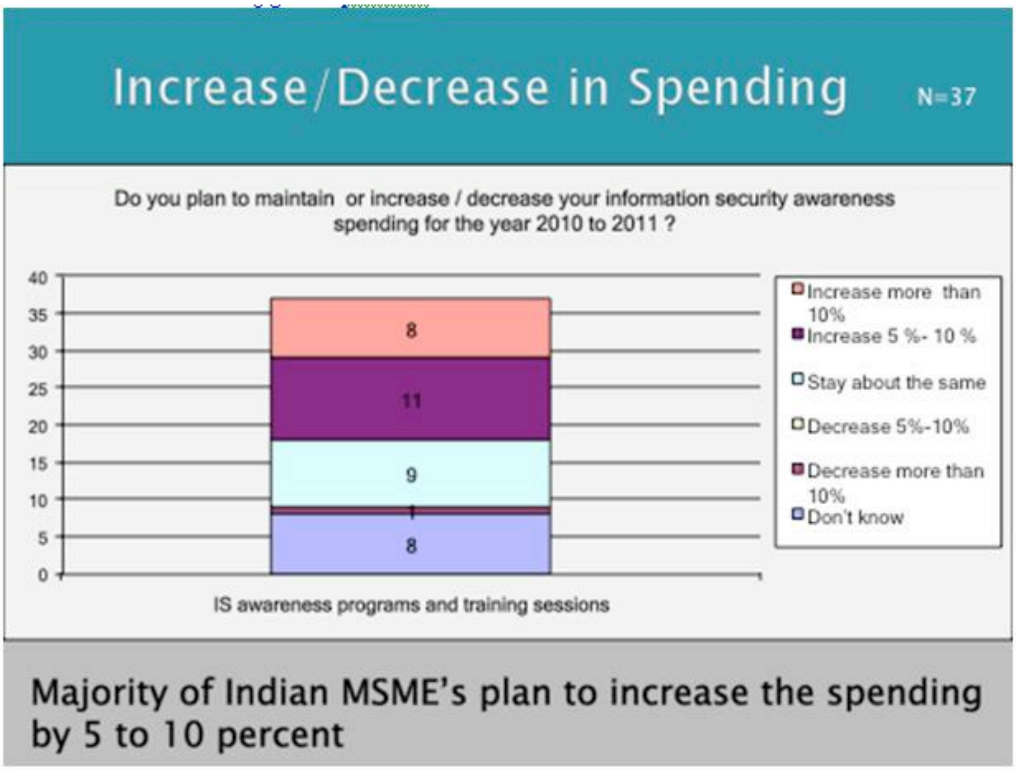
Which of the following proportions of your company's IT budget is allocated for information security awareness ?

Majority Indian SME's have separate budget for security awareness

Figure 46: Proportion of IT Budget for Awareness in Indian MSME's

Majority of participants from IT, Financial services state that their organization have separate budget for security awareness and training programs. 40 percent of participants from financial services state that they spend 1 to 5 of IT budget for security awareness. Majority of participants from micro and medium have separate budget for security awareness.

30 percent or Majority of participants state that their organizations would like to increase the investment by 5 to 10 percent .



Increase/Decrease in Spending N=37

Do you plan to maintain or increase / decrease your information security awareness spending for the year 2010 to 2011 ?

Majority of Indian MSME's plan to increase the spending by 5 to 10 percent

Figure 47: Increase /Decrease in spending in Indian MSME's

MSME organizations from IT, financial services and other industry sectors participants state that their spending on security awareness and training programs to increase by 5 to 10 percent .18.8 percent of participants from IT, financial services and other industry sector state that they would like to increase greater than 10 percent. Whereas 31.3 percent of participants from IT, pharmaceuticals and other industry sector state that their organization security awareness investment will remain the same. Majority or 45 percent of participants from medium, 10 percent from small, 20 percent from micro state that they would like to increase their spending by greater than 5 to 10 percent.

5 Comparing the results

In this section, we compare the results of different industry sector IT , Financial services , Pharmaceuticals , Government & public sector and other industry sector participants

5.1.1 Comparison on IT Industry Sector

COMPARISON ON IT INDUSTRY SECTOR		
FOCUS AREAS	**NORWAY**	**INDIA**
Managing Information Security	Confidentiality is top security goal 62.5 percent state staff with secondary job function 71% have Security Policies ,out of which 50 Percent state that they are accessible Driver for Security policy is improved business practices 50 % state security policy is measured All are maintaining antivirus , firewall, spam filter , back up , with few not following good password practices Employees are greatest threat	Confidentiality is top security goal 64.7 percent state staff with secondary job function 76.5% have Security Policies ,out of which 43.8% state that they are accessible Driver for Security policy is improved business practices 56.3 % state security policy is measured All are maintaining antivirus , firewall and back up , with few not maintaining spam filter ,good password practices Employees using personal email are greatest threat
Security Culture	Top Management is convinced that IS is important Investment is making a difference for improving security culture	Top Management is convinced that IS is important Insufficient budget is an Inhibiting factor Investment is making a difference for improving security culture
Security Awareness	57.1% do every 6,12 and 2 years 28.6 % state review and agreement of compliance with current security policy and standards,14.3 % incidence reporting as elements for security awareness and training programs Employee Non Seriousness is an Inhibiting factor	41.2 % do them every 6 months 56.3 % state review and agreement of compliance with current security policy and standards,50 % general IS awareness topics as elements for security awareness &training programs Workshops for employees is

	Web portal is widely used security awareness campaigns Web portal is widely used security awareness campaigns in next 2 years 71.4 % state no separate budget 71% state stay the same	widely used security awareness campaigns Workshops for employees, web portal is widely used security awareness campaigns in next 2 years 64.7 have separate budget Majority plan to increase by greater than 5 and more

Table 6: COMPARISON ON IT INDUSTRY SECTOR

5.1.2 Similarities and Differences in IT Industry Sector

The organizations from Norwegian and Indian IT MSME's have similar top priority security goals for their organizations .The results gives me an impression that confidentiality is stated as their top priority security goal basing on the fact that their organizations have personal data and critical important information about of their customers, which they feel is their top priority security goal goals compared to availability, integrity and traceability.

Organisation structure of Managing Information Security is similar in Norwegian and Indian IT MSME's . Both Norwegian and Indian MSME's are having staff with secondary job function for managing information security. But overall results show that information security is not managed well in Indian IT MSME's as some of participants do have security policies, some even though they have security policies are not completely accessible to employees. Some of MSME's do not even have firewalls, anti spam filter, regular back of up of data; maintain good password practices to protect computer and electronic data. This gives an impression that staff with secondary job function for managing information security are not well qualified or knowledgeable to manage information security or the employees are not serious as results stated or the top management is not measuring the information security staff performance or supporting for the improvement of information security.

The results show that Norwegian and Indian IT MSME's top management is convinced that information security is important for achieving the business objectives, but revealed also some main weaknesses in security culture of Norwegian and Indian IT MSME's. Norwegian and Indian IT enterprises culture shows employees are not serious on security and have lack of right people to run the awareness activities in house with additional Indian IT enterprises stating insufficient budget as the main weaknesses.

Security awareness and training programs are more frequently done in Norwegian IT enterprises compared to Indian enterprises even though majority Norwegian enterprises do not have separate budget for security awareness. On another hand Indian MSME's are having more proportion of budget and plan to spend more in 2010-11 for security awareness compared to Norwegian enterprises. But the weaknesses in Indian enterprises with respect to the security culture, awareness and managing information security shows that the budget is not utilised properly and effectively for creating more information security awareness. The different regions also have different priorities of elements covered in the security awareness and training programs. A detailed analysis of elements covered showed that more effort should be out on improving the security awareness in Indian MSME's with respect to incidence reporting and direct & frequent updates/alerts on current threats to their organization as majority elements covered in security training are on general information security topics. Web portal are widely in Norwegian MSME's , whereas Indian enterprises state workshops for employees as mainly used security campaigns for their organizations .This also shows that there is need better channels and security awareness solutions needed to create security awareness campaigns in Indian IT enterprises compared to Norwegian enterprises.

5.2.1 Comparison on Financial Services Industry Sector

COMPARISON ON FINANCIAL SERVICES INDUSTRY SECTOR		
FOCUS AREAS	**NORWAY**	**INDIA**
Managing Information Security	Availability is top security goal 66.7 percent state have dedicated staff All have security policy ,out of which everyone is able to access Driver for Security policy is legislative regulations 66.7 % state security policy is measured All maintain antivirus , firewall, spam filter , back up , and good password practices Competitors are greatest threat	Confidentiality is top security goal 66.7 percent state have dedicated staff 75% have security policy , out of which 40% state that they are accessible Driver for Security policy is legislative regulations, improved business practices, auditing regulations and security breaches 60 % state security policy is measured All are maintaining antivirus ,but there is also around 40% not maintaining firewall ,back up ,spam filter and good password practices Ex-Employees are greatest threat

Security Culture	Top Management is convinced that IS is important Lack of Management Support is an Inhibiting factor Majority state investment is making a difference for improving security culture	Top Management is convinced that IS is important Employee Non Seriousness is an Inhibiting factor Investment is making a difference for improving security culture
Security Awareness	Equally do SAP every 6,12 and 24 months All state review and agreement of compliance with current security policy and standards and incidence reporting as elements for security awareness and training programs Workshops for management is widely used security awareness campaigns Workshops for management is widely used security awareness campaigns in next 2 years 33.3 state 3 to 5% budget and rest no budget 66.7% state stay the same	40% every 6 months 60% general IS awareness topics,60 % alerts on current threats, measuring effectiveness of IS,40% incidence reporting as elements for security awareness &training programs Newsletters is widely used security awareness campaigns Posters , Newsletters , quizzes & games is widely used security awareness campaigns in next 2 years Majority state 1 to 5 percent budget 80% state increase more than 5%

Table 7: COMPARISON ON FINANCIAL SERVICES INDUSTRY SECTOR

5.2.2 Similarities and Differences on Financial Services Industry Sector

The organizations from Norwegian and Indian financial services MSME's have dissimilar priority security goals for their organizations. Norwegian enterprises state data availability as top priority security goal, whereas Indian enterprises state confidentiality as their top priority security goal. The results of Norwegian enterprises gives me an impression that availability is stated as their top priority security goal basing on the fact that their organizations are mainly looking for the immediate survival of the business or more towards offering best services to their customers. Whereas Indian enterprises state confidentiality giving more priority to personal data and critical information assets they have about their customers and secondly it also gives me impression that they are less focussed on offering better customer satisfaction services to customers by making the data available.

Organisation structure of Managing Information Security is similar in Norwegian and Indian financial services MSME's. Majority of MSME's in Norway and India are having dedicated staff to manage information security. But overall results show that information security is not managed well in Indian financial services MSME's as some of participants do have security policies, some even are not completely accessible to employees. Some of the participants do not even have firewalls, anti spam filter, regular back of up of data; maintain good password practices to protect computer and electronic data. This also gives an impression that the dedicated staff for managing information security are not well qualified to manage information security or the top management is not measuring the information security staff on their performance or supporting for the improvement of information security in their organizations.

The Norwegian and Indian financial services MSME's top management is convinced that information security is important for achieving the business objectives, but revealed also some weaknesses in security culture of Norwegian and Indian enterprises. Norwegian enterprises culture shows are Lack of management support, organisation culture, employees not serious on security and have lack of right people to run the awareness activities in house, Whereas Indian enterprises culture shows employee not serious, lack of management support and insufficient budget the weaknesses.

Security awareness and training programs are more frequently done in Norwegian enterprises compared to Indian enterprises even though majority enterprises do not have separate budget for security awareness. On another hand Indian MSME's are having more proportion of budget and plan to spend more in 2010-11 for security awareness compared to Norwegian enterprises. The different regions have different priorities of elements covered in the security awareness and training programs .Workshops for management are widely in Norwegian MSME's , whereas Indian enterprises state newsletter as mainly used security campaigns for their organizations .This also shows that there is need better channels and security awareness solutions needed to create security awareness campaigns in Indian IT enterprises for raising security awareness.

Overall, the information security maturity levels in Norwegian financial services MSME's is good compared to Indian enterprises with respect to the managing of information security and awareness.

5.3.1 Comparison on Pharmaceutical Industry Sector

In this part, we do not have participants for the Norwegian Survey and we have stated the results of India

COMPARISON ON PHARMACEUTICAL INDUSTRY SECTOR		
FOCUS AREAS	**NORWAY**	**INDIA**
Managing Information Security	No Participants	Confidentiality is top security goal 16.7% state have dedicated staff,16.7% non dedicated,33,3 outside experts for managing IS 40% have security policy, out of which 20% accessible Driver for Security policy is improved business practices, auditing regulations and external security breaches 80 % state security policy is not measured All are maintaining antivirus ,but few do not have firewall and back up and 50% do not even maintain spam filter and good password practices Competitors are greatest threat
Security Culture	No Participants	Top Management is convinced that IS is important Lack of Right People as inhibiting factor Investment is making a difference for improving security culture
Security Awareness	No Participants	83.3% do not do them at all 20 % state review and agreement of compliance with current security policy and standards,40 % general IS awareness topics as elements for security awareness &training programs Brochures & flyers is widely used security awareness campaigns Workshops for employees is widely used security awareness campaigns in next 2 years 50% have no separate budget 1/3 state would increase more than 5%

Table 8:COMPARISON ON PHARMACEUTICAL INDUSTRY SECTOR

5.3.2 Similarities and Differences on Pharmaceutical Industry Sector

The organizations from Indian pharmaceutical MSME's state confidentiality as their top priority security goals for their organizations . The results of Indians enterprises gives me an impression that confidentiality is stated as their top priority security goal basing on the fact that their organizations are mainly looking giving more priority to personal data and critical information assets they have about their customers compared to availability, integrity and traceability of data.

Organisation structure of Managing Information Security in Indian pharmaceutical MSME's is done through dedicated staff, on dedicated staff . But overall results show that information security is not managed well in Indian pharmaceutical MSME's as some of majority do have security policies and majority of them are not completely accessible to employees. Some of the participants do not even have firewalls, anti spam filter, regular back of up of data; maintain good password practices to protect computer and electronic data. This also gives an impression that the dedicated or non dedicated staff for managing information security are not well qualified or knowledgeable to manage information security or the top management is not measuring the information security staff on their performance or supporting for the improvement of information security in their organizations.

The Indian pharmaceutical MSME's top management is convinced that information security is important for achieving the business objectives, but revealed also some weaknesses in security culture. Indian enterprises culture shows lack of right people to run the awareness activities as the main weaknesses.

Security awareness and training programs are also not frequently done in Indian and majority are do not even have plan to allocate budget for security awareness and training programs. Brochures and flyers are widely used security campaigns for their organizations .This also shows that there is need better channels and security awareness solutions needed to create security awareness campaigns in their organizations.

Overall, the information security maturity levels in Indian pharmaceutical MSME's is not good with respect to the managing of information security, culture and awareness.

5.4.1 Comparison on Government and Public Industry Sector

COMPARISON ON GOVT&PUBLIC SECTOR

FOCUS AREAS	**NORWAY**	**INDIA**
Managing Information Security	Availability is top security goal 66.7% participants state staff with secondary job function for managing IS All have Security policy ,out of which 66.7% state that they are accessible Driver for Security policy is improved business practices, legislative regulations and protection of brand and image 66.7 % state security policy is not measured All maintain antivirus , firewall and back up , whereas only 33.3% maintain spam filter and good password practices Employees andmalware are greatest threat	Availability is top security goal Equally participants state have dedicated staff, on dedicated, outside experts for managing IS 66.7 have security policy ,out of which 50 percent accessible Driver for Security policy is external security breaches 50 % state security policy is measured All are maintaining antivirus ,but majority are not having back up ,good password practices Employees using personal email,malware and spam are greatest threat
Security Culture	Top Management and Employees are convinced that IS is important Fear and Resistance to Change from employees the top inhibiting factor Yes some state investment is worth and some state investment is worth but not making a difference for improving security culture	Top Management is convinced that IS is important Lack of management support and right people to run the activities the top inhibiting factor Yes Majority state investment is worth, but not making a difference for improving security culture
Security Awareness	66.7% do not do them at all General IS awareness topics and incidence reporting as elements for security awareness &training programs Web portal is widely used security awareness campaigns	33% every 2 yrs,33% do not do at all 66.7 % general IS awareness topics and incidence reporting as elements for security awareness &training programs Workshops for management

	Web portal is widely used security awareness campaigns in next 2 years 67% have no separate budget 33.3 increase more than 10%	&employees ,brochures& flyers is widely used security awareness campaigns Workshops for management & employees is widely used security awareness campaigns in next 2 years 66.7% have no separate budget All say do not know

Table 9: COMPARISON ON GOVT&PUBLIC SECTOR

5.4.2 Similarities and Differences on Government and Public Industry Sector

The organizations from Norwegian and Indian financial services MSME's have similar priority security goals for their organizations. Norwegian and Indian enterprises state data availability as top priority security goal. This gives us an impression that availability is stated as their top priority security goal basing on the fact that their organizations are mainly looking for offering best services to their general public. .

Organisation structure of Managing Information Security is not similar in Norwegian and Indian IT MSME's. Majority of MSME's in Norway have staff with secondary job function for managing information security, whereas Indian enterprises have dedicated staff, non dedicated staff and outside experts for managing information security. But overall results show that information security is well managed in Norway with everyone implementing of security policies for improved business practices and based on legislative regulations and also reflecting the fact that the staff with secondary job function for information security are well qualified and are performing their duty of managing information security well, Whereas Indian enterprises are not managing information security well compared to Norwegian enterprises as some of participants do have security policies, some security policies even are not completely accessible to employees. Some of the participants do not even have regular back of up of data and maintain good password practices to protect computer and electronic data. This also gives an impression that the dedicated and non dedicated staff and outside experts for managing information security are not well qualified to manage information security or the top management is not measuring the information security staff on their performance or supporting for the improvement of information security in their organizations.

The Norwegian and Indian IT MSME's top management is convinced that information security is important for achieving the business objectives, but revealed also some weaknesses in security culture of Norwegian and Indian Government & public sector MSME's . Norwegian enterprises culture shows employees not serious on security,

insufficient budget and have lack of right people to run the awareness activities in house, Whereas Indian IT enterprises culture shows that their lack of management support, employees are not serious and fear and resistance to change from employees the weaknesses.
Norwegian and Indian Government & public sector enterprises are almost similar security awareness and training programs. Both Norwegian and Indian enterprises have same priorities of elements covered in the security awareness and training programs. Web portals are widely in Norwegian MSME's , whereas Indian enterprises state workshops for employees, management ,brochures & flyers as mainly used security campaigns for their organizations. This also shows that there is need better channels and security awareness solutions needed to create security awareness campaigns in Indian government & public sector enterprises for raising security awareness as the security culture need to improved.

Overall, the information security maturity levels in Norwegian Government & Public sector MSME's is good compared to Indian enterprises with respect to the managing of information security and awareness.

5.5.1 Comparison on Other Industry Sector

COMPARISON ONOTHER INDUSTRYSECTORS		
FOCUS AREAS	**NORWAY**	**INDIA**
Managing Information Security	Confidentiality, Availability is top security goal 33.3% participants state staff with dedicated staff ,33.3 % state secondary job function for managing IS All have security policy ,out of which 83.3 state that they are accessible Driver for Security policy is improved business practices 66.7 % state security policy is measured All maintain antivirus , firewall and good password practices ,whereas few do not maintain spam filter and back up Employees are greatest threat	Confidentiality is top security goal 62.5% participants state staff with secondary job function for managing IS 62% have security policy ,out of which 14.3 percent accessible Driver for Security policy is improved business practices 71.4 % state security policy is measured All maintain antivirus and some do not even maintain firewalls, spam filters , password practices and back up Malware and employees using personal email the greatest threat

Security Culture	Top Management are convinced that IS is important 33.3 state investment is not worth for improving security culture	Top Management are convinced that IS is important Employee Non Seriousness the top inhibiting factor 83.3 state investment is worth for improving security culture
Security Awareness	All of them do once a year General IS awareness topics, review and agreement of compliance with current security policies and standards and incidence reporting as elements for security awareness &training programs Lack of right people to run the activities the top inhibiting factor Web portal, newsletters is widely used security awareness campaigns Posters, Web portal is widely used security awareness campaigns in next 2 years 33.3 % have no separate budget and 50% don't know 60 Remain the same on spending	50% do not do them at all,50% do them every 6,12 months 66.7 % general IS awareness topics and incidence reporting as elements for security awareness &training programs Workshops for employees is widely used security awareness campaigns E learning is widely used security awareness campaigns in next 2 years 33.3% have greater than 5% of budget 62% state increase more than 5% on spending

Table 10:COMPARISON ON OTHER INDUSTRYSECTORS

5.5.2 Similarities and Differences on Other Industry Sector

The organizations from Norwegian and Indian other industry sector MSME's have similar priority security goals for their organizations with respect to confidentiality of information, whereas Norwegian enterprises also state availability as their top priority. Norwegian enterprises and Indian enterprises state confidentiality as top priority security goal. The results gives me an impression that confidentiality is stated as their top priority security goal basing on the fact that their organizations have personal data and critical important information about of their customers, which they feel is their top priority security goal .On another hand results of Norwegian enterprises state that availability also their top priority security goal giving us an impression that they are mainly looking for offering best services to their general customers.

Organisation structure of Managing Information Security is not similar in Norwegian and Indian IT MSME's . Majority of MSME's in Norway have dedicated staff, non dedicated staff and outside experts for managing information security, whereas Indian enterprises have non dedicated staff for managing information security. But overall results show that information security is well managed in Norway with everyone implementing of security policies for improved business practices and for legislative regulations, Whereas Indian enterprises are not able to manage well compared to Norwegian enterprises as some of participants do have security policies, some security policies even are not completely accessible to employees. Indian enterprises state improved business practices and auditing regulations as the drivers for creation of security policy. Some of the Indian participants do not even have firewalls, anti spam filters, regular back of up of data and maintain good password practices to protect computer and electronic data . This also gives an impression that the people for managing information security are not well qualified to manage information security or the top management is not measuring the information security staff on their performance or supporting for the improvement of information security in their organizations.

The Norwegian and Indian MSME's top management is convinced that information security is important for achieving the business objectives, but revealed also some different weaknesses in security culture of Norwegian and Indian other sector MSME's . Norwegian enterprises culture show lack of right people to run the awareness activities in house, fear and resistance to change from employees and organisation culture , Whereas Indian IT enterprises culture shows employees are not serious on security, organisation culture and lack of right people to run the awareness activities in house the weaknesses.

Security awareness and training programs are more frequently done in Norwegian enterprises compared to Indian enterprises even though majority enterprises do not have separate budget for security awareness. On another hand Indian MSME's are having more proportion of budget and plan to spend more in 2010-11 for security awareness compared to Norwegian enterprises. Also both Norway and Indian enterprises have similar priorities of elements covered in the security awareness and training programs like general information security awareness topics and incidence reporting. This also shows that there is need better channels and security awareness solutions needed to create security awareness campaigns in Indian government & public sector enterprises for raising security awareness as the security culture need to improved.

Overall, the information security maturity levels in Norwegian other sector MSME's is good compared to Indian enterprises with respect to the managing of information security and awareness.

5.6.1 Comparison on Micro Enterprises

Comparisons on Size of Enterprises		
Micro	**NORWAY**	**INDIA**
Managing Information Security	Integrity is top security goal 25 Percent for dedicated staff, secondary and outside experts for managing IS 66.7 Percent have security policy and are state that they are accessible Driver for Security policy is legislative regulations 66.7 % state security policy is measured is not known All maintain antivirus ,firewall,anti spam filter ,regular back up and whereas few do not have good password practices . Employees are the greatest threat	Confidentiality, Availability is top security goal 66.7 Percent have staff with secondary job function for managing IS 50 Percent have security policy out of which 25 percent state that they are accessible Driver for Security policy is improved business practices 50 % state security policy is not measured All maintain antivirus ,firewall, regular back up and whereas few do not maintain good password practices ,anti spam filters Competitors are the greatest threat
Security Culture	Top Management are convinced that IS is important Fear and resistance to change from employees, Insufficient budget and Lack of right people to run the activities the top inhibiting factor	Top Management are convinced that IS Insufficient budget and Lack of right people to run the activities the top inhibiting factor
Security Awareness	67 percent do once a year Mostly review and agreement of compliance with security policy and incidence reporting as elements for security awareness &training programs Posters is widely used security awareness campaigns Posters is widely used security awareness campaigns in next 2 years	67 do not do them at all 80 % state general IS awareness topics as elements for security awareness &training programs Mix of answers on budget 60 Stay the same Articles in Newspapers is widely used security awareness campaigns Blogs, Social Networks is widely used security awareness

	33.3 no separate budget, Whereas another 33.3 state don't know All Stay the same	campaigns in next 2 years

Table 11: Comparison on Micro Enterprises

5.6.2 Similarities and Differences on Micro Enterprises

The organizations from Norwegian and Indian micro enterprises have dissimilar priority security goals for their organizations. Norwegian enterprises state integrity as top priority security goal, whereas Indian enterprises state confidentiality, availability as their top priority security goal. The results of Norwegian enterprises gives me an impression that integrity is stated as their top priority security goal basing on the fact that their organizations are mainly looking for the moral and ethical principles and honesty way for their survival of the business . Whereas Indian enterprises state confidentiality, availability. This gives us an impression that confidentiality, availability are stated as their top priority security goal basing on the fact that their organizations are mainly looking for offering best services to their customer and at the same time are looking for security their or customer personal data confidentially.

Organisation structure of Managing Information Security is not similar in Norwegian and Indian Micro Enterprises . Majority of Micro enterprises in Norway have dedicated staff, non-dedicated staff and outside experts for managing information security, whereas Indian enterprises have non-dedicated staff for managing information security. But overall results show that information security is well managed in Norway with majority implementing of security policies mainly for legislative regulations, Whereas Indian MSME's not managed well as half of participants do have security policies and again half of these security policies even are not completely accessible to employees. Some of the Indian participants do not maintain good password practices and anti spam filters to protect computer and electronic data. . This also gives an impression that the people for managing information security are not well qualified to manage information security or the top management is not measuring the information security staff on their performance or supporting for the improvement of information security in their organizations.

The Norwegian and Indian enterprises top management is convinced that information security is important for achieving the business objectives, but revealed also some different weaknesses in security culture of Norwegian and Indian other sector enterprises. Norwegian enterprises culture show fear and resistance to change from employees, organisation culture and lack of sufficient budget, Whereas Indian IT enterprises culture shows Lack of sufficient budget, lack of right people to run the awareness activities in house and employee non seriousness the main weaknesses.

Security awareness and training programs are more frequently done in Norwegian enterprises compared to Indian enterprises even though majority enterprises do not have separate budget for security awareness. Also both Norwegian and Indian enterprises have different priorities of elements covered in the security awareness and training programs. Indian enterprises cover general awareness topics, whereas Norwegian enterprises cover review and agreement of security policy and incidence reporting. This also shows that there is need better channels and security awareness solutions needed to create security awareness campaigns in Indian micro enterprises for raising security awareness as the security culture need to improved.

Overall, the information security maturity levels in Norwegian Micro Enterprises is good compared to Indian enterprises with respect to the managing of information security and awareness.

5.7.1 Comparison on Small Enterprises

Comparisons on Size of Enterprises		
Small	**NORWAY**	**INDIA**
Managing Information Security	Confidentiality, Availability is top security goal 43 Percent have dedicated staff and another 43 state staff with secondary job function for managing IS 85.7 Percent have Security policy ,out of 83.3 Percent state that they are accessible Driver for Security policy is improved business practices 50% state security policy is measured All maintain antivirus, firewall, good password practices and whereas few do not have anti spam filter and regular back up. Employees are the greatest threat	Confidentiality is top security goal 70 percent state staff with secondary job function 66.7 Percent have security policy , out of which 33.3 percent state that they are accessible Driver for Security policy is improved business practices 70% state security policy is not measured All maintain antivirus, firewall, regular back up ,but majority do not even maintain good ,anti spam filter Competitors are the greatest threat
Security	Top Management are convinced	Top Management are convinced

Culture	that IS is important Employee Non Seriousness the top inhibiting factor	that IS is important Employee Non Seriousness the top inhibiting factor
Security Awareness	Majority do every 6 ,12 months and every 2 years Majority state review and agreement of compliance with security policies and incidence reporting as elements for security awareness &training programs Web portal is widely used security awareness campaigns Workshops for employees the widely used security awareness campaigns in next 2 years 57.1 % no separate budget 71 Percent stay same on spending	40 percent do not do them at all and 50 percent do every 6,12 months and 2 years 44.4 % state general IS awareness topics and review and agreement of compliance with security policies as elements for security awareness &training programs Articles in Newspapers is widely used security awareness campaigns Workshops for employees the widely used security awareness campaigns in next 2 years 50 Percent no separate budget 40 Percent or majority remain the same

Table 12:Comparisons on Size of Enterprises

5.7.2 Similarities and Differences on Small Enterprises

The organizations from Norwegian and Indian micro enterprises have dissimilar priority security goals for their organizations. Norwegian enterprises state confidentiality, availability as top priority security goal, whereas Indian enterprises state confidentiality as their top priority security goal. The results of Norwegian enterprises gives me an impression that confidentiality, availability is stated as their top priority security goal basing on the fact that their organizations are mainly looking for offering best services to their customer and at the same time are looking for security their or customer personal data confidentially. Whereas Indian enterprises state confidentiality .This gives us an impression that confidentiality is stated as their top priority security goal basing on the fact that their organizations are mainly looking for security of their or customer and personal data .

Organisation structure of Managing Information Security is not similar in Norwegian and Indian Small Enterprises . Majority of Small enterprises in Norway have dedicated staff, non-dedicated staff for managing information security, whereas Indian enterprises have non-dedicated staff for managing information security. But overall results show that information security is well managed in Norway with majority implementing of security policies mainly for improved business practices, Whereas some of these Indian Micro enterprises do not security policies and again half of these security policies even are not completely accessible to employees. Some of the Indian participants do not maintain good password practices and anti spam filters to protect computer and electronic data. This also gives an impression that the people for managing information security are not well qualified to manage information security or the top management is not measuring the information security staff on their performance or supporting for the improvement of information security in their organizations.

But the results show that Norwegian and Indian MSME's top management is convinced that information security is important for achieving the business objectives, but revealed also some different weaknesses in security culture of Norwegian and Indian other sector MSME's . Norwegian enterprises culture show Employees are not serious, lack of right people to run the awareness activities in house and lack of sufficient budget, Whereas Indian IT enterprises culture shows employees are not serious on security, lack of management support and organisation culture the main weaknesses.

Security awareness and training programs are more frequently done in Norwegian small enterprises compared to Indian enterprises even though majority enterprises in both regions do not have separate budget for security awareness. Also both Norway and Indian enterprises have different priorities of elements covered in the security awareness and training programs except review and agreement of security policy. This also shows that there is need better channels and security awareness solutions needed to create security awareness campaigns in Indian small enterprises for raising security awareness as the security culture need to improved.

Overall, the information security maturity levels in Norwegian small Enterprises is good compared to Indian enterprises with respect to the managing of information security and awareness.

5.8.1 Comparison on Medium Enterprises

Comparisons on Size of Enterprises		
Medium	**NORWAY**	**INDIA**
Managing Information Security	Availability is top security goal 75 percent state staff with secondary job function for managing IS All have security policy ,out of which 62.5 percent state that they are accessible	Confidentiality is top security goal 47.6 percent dedicated staff and 33.3 state staff with secondary job function for managing IS 70 percent have security policy ,out which only 35 percent state they are accessible

	Driver for Security policy is improved business practices, Legislative and auditing regulations, protection of brand & image and industry standards 62.5 % state security policy is not measured All maintain antivirus, firewall, regular back up and whereas ¼ say they do not have anti spam filter and good password practices. Employees are the greatest threat	Driver for Security policy is improved business practices, 63.2 % state security policy is measured All maintain antivirus ,but some companies do not even maintain firewalls, anti spam filters, regular back up and good password practices . Employees using personal emails ,malware are the greatest threat
Security Culture	Top Management are convinced that IS is important Lack of right people to run the awareness activities the top inhibiting factor	Top Management are convinced that IS is important Employee Non Seriousness and lack of management support the top inhibiting factor
Security Awareness	62.5 Percent every 6,12 months Majority state general IS awareness topics ,review and agreement of compliance with security policies and incidence reporting as elements for security awareness &training programs Web portal is widely used security awareness campaigns Web portals the widely used security awareness campaigns in next 2 years 62.5 no separate budget 50 Percent same on spending	Majority do them every 6,12 and 2 ,3 years 47.6 % state general IS awareness topics and review and agreement of compliance with security policies and incidence reporting as elements for security awareness &training programs Web portal is widely used security awareness campaigns Workshops for employees the widely used security awareness campaigns in next 2 years Majority have separate budget between 1 to 5 % 65 Percent increase greater than 5 percent

Table 13: Comparisons on Medium Enterprises

5.8.2 Similarities and Differences on Medium Enterprises

The organizations from Norwegian and Indian micro enterprises have dissimilar priority security goals for their organizations. Norwegian enterprises state availability as top priority security goal, whereas Indian enterprises state confidentiality as their top priority security goal. The results of Norwegian enterprises gives me an impression that availability is stated as their top priority security goal basing on the fact that their organizations are mainly looking for offering best services to their customers . Whereas Indian enterprises state confidentiality . This gives us an impression that confidentiality is stated as their top priority security goal basing on the fact that their organizations are mainly looking for security of their or customer and personal data .

Organisation structure of Managing Information Security is not similar in Norwegian and Indian Small Enterprises . Majority of Medium enterprises in Norway have non-dedicated staff for managing information security, whereas Indian enterprises have dedicated and non-dedicated staff and outside experts for managing information security. But overall results show that information security is well managed in Norway with majority implementing of security policies mainly for improved business practices, legislative regulations, industry standards etc, Whereas majority of Indian medium enterprises have security policies and again half of these security policies even are not completely accessible to employees. Some of the Indian participants do not maintain firewalls , anti spam filters, regular back up of data and good password practices to protect computer and electronic data. This also gives an impression that the people for managing information security are not well qualified to manage information security or the top management is not measuring the information security staff on their performance or supporting for the improvement of information security in their organizations.

The Norwegian and Indian Medium enterprises top management is convinced that information security is important for achieving the business objectives, but revealed also some different weaknesses in security culture of Norwegian and Indian Medium enterprises. Norwegian enterprises culture show show lack of right people to run the awareness activities in house, employees are not serious on security, organisation culture and fear & resistance to change from employees, Whereas Indian enterprises culture show employees are not serious, lack of sufficient budget and lack of right people to run the awareness activities in house the main weaknesses.

Security awareness and training programs are different in Norwegian and Indian medium enterprises. Majority of security awareness and training programs are more in Indian enterprises. Both Norwegian and Indian enterprises have similar elements covered in the security awareness and training programs like general information security awareness topics, review and agreement of security policy and incidence reporting. The results show that Indian medium enterprises are planning to spend more on security awareness compared to Norwegian enterprises.

Overall, the information security maturity levels in Norwegian Medium Enterprises is slightly better compared to Indian enterprises with respect to the managing of information security and awareness.

6 Conclusions and Recommendations

1.The security culture, awareness and managing information security is at a very good level in Norwegian financial service enterprises.

2.Information Security Maturity levels in Norwegian MSME's is high compared to Indian MSME's with respect to managing of information security and awareness .

A. MSME's in Norway and India are having dedicated, non-dedicated staff and outside experts to manage information security ,but managing information security is not similar in both the regions. Information Security is well managed in Norwegian MSME's with having qualified staff for managing information security .Whereas information security is not managed well in Indian MSME's due to lack of qualified experts or employee non seriousness . It is recommended that Information security management should be improved in Indian MSME's by recruiting qualified security persons for managing information security through proper implementation of security policies, accessibility to employees and measuring them and taking measuring to protect computer & electronic data.

B. Norwegian and Indian MSME's have different drivers for creation of security policy. A analysis of drivers for creation of security policy in India shows that there is not given much importance for Indian legislative regulations and standards. Indian government should put in effort to identify the weakness in the legislative regulations and make the legislative regulations more visible and standards stronger. So that Indian MSME'smake information security as their top priority security goal achieving their business objectives and managing information security well in their organizations.

C. The Norwegian and Indian MSME's top management is convinced that information security is important for achieving the business objectives, but revealed also some main weaknesses in security culture in like Employee Non Seriousness, lack of right people to run the awareness activities in house, organisation culture and fear and resistance to change from employees. These weaknesses should be improved. Most effort should be to put on Training & Education for employees who are not serious and fear & resistance to change with run people to run awareness activities. Also making the security experts more visible will also positively influence the security culture of Norwegian and Indian MSME's.

D. The Norwegian and Indian MSME's have different priorities of elements covered in the security awareness and training programs. A detailed analysis of elements covered showed that more effort should be out on improving the security awareness in Indian MSME's with respect to incidence reporting and direct & frequent updates/alerts on current threats to their organization. The different regions also different proportions of budget allocated for information security awareness. A detailed analysis shows that Indian MSME's are having more proportion of budget and plan to spend more in 2010-11 for security awareness compared to Norwegian enterprises. But the weaknesses in Indian enterprises with respect to the security culture, awareness and managing information security shows that that their of right people to run the awareness activities and for managing information security. Qualified staff and well-established budget plan is recommended for the Indian MSME's with improving the security awareness with their organizations.

E. Overall, the information security maturity levels in Norwegian MSME's is good compared to Indian enterprises with respect to the managing of information security, security culture and awareness.

7 Future work

As this study is mainly a quantitative study, it is important to note that true maturity levels may not be measured accurately by a questionnaire alone, as respondents do not necessarily tell the truth when asked about their enterprise maturity levels on people factor. The measuring process used in this is not supported by personal interviews (or qualitative study) to verify if the online survey results match. It is recommended if a study with a combination of qualitative and quantitative study is done to see if the results match with equal number of participants in the target groups.

8 Bibliography

[1] David Lacey, 2009.Managing the Human Factor in Information Security.

[2] Deloitte, 2009.The 6th Global information security survey. Electronic version found at http://www.deloitte.com/assets/Dcom-Luxembourg/Local%20Assets/Documents/Surveys/dtt_globalsecuritysurvey_012009.pdf

[3] Detecon (Schweiz) AG. The Value of Information Security to European Banking Institutions . Electronic Version found at personal.lse.ac.uk/LIEBENAU/BankingSecurityDETECOM.doc

[4] Devoteam Consulting, 2008.International Information Systems Security Survey. Electronic version found at http://www.devoteam.com/images/File/SecuritySurvey-BD.pdf

[5] DojkovskiSneza , Lichentenstein Sharman, Warren Mathew John (2006) . Fostering Information Security Culture in Small and Medium Size Enterprises. Electronic version found at http://is2.lse.ac.uk/asp/aspecis/20070041.pdf

[6] Dr.Thomas Schlienger, Tree Solution Consulting Gmbh www.treesolution.ch

[7] Dr.Thomas Schlienger , Tree Solution Consulting Gmbh, 2008.Survey on Information Security Culture in Swiss Companies

[8] DSCI –KPMG Survey, 2009.State of Data Security and Privacy in the Indian Industry . Electronic Version found at http://www.dsci.in/sites/default/files/data_security_survey_2009_report_final_30th_dec_2009.pdf

[9] Ernst &Young, 2010. Outpacing Change: 12th Annual Global Information Security Survey. Electronic version found at http://www.ey.com/Publication/vwLUAssets/12th_annual_GISS/$FILE/12th_annual_GISS.pdf

[10] European Network and Information Security Agency, 2006.A user guides: How to raise information security awareness. Electronic version found at http://www.enisa.europa.eu/act/ar/deliverables/2006/ar-guide/en

[11] European Network and Information Security Agency, 2008.Awareness Raising Quiz templates for parents, end users and SME . Electronic version found at http://www.enisa.europa.eu/act/ar/deliverables/2008/ar-quizzes-templates-en

[12] European Network and Information Security Agency document on Compilation and Dr..Thomas Schlienger, 2009.The AR Conference Calls .Electronic version found at http://www.enisa.europa.eu/act/ar/deliverables/2008/compilation-the-ar-conference-calls-2008

[13] European Network and Information Security Agency, 2009.Growing requirement for information security awareness. Electronic version found at http://www.enisa.europa.eu/act/ar/deliverables/2009/ar-book-09

[14] European Network and Information Security Agency, 2008.Information Security Awareness in financial organisations .Electronic version found at http://www.enisa.europa.eu/act/ar/deliverables/2008/is-in-financial-organisations

[15] European Network and Information Security Agency, 2008.Security Awareness Management in Local Government: Approaches in Scandinavia .Electronic version found at http://www.enisa.europa.eu/act/ar/deliverables/2008/scandinavian-approaches-survey

[16] H.A Kruger and W.D Kearney, 2006.A prototype for assessing information security awareness .Electronic version found at http://www.puk.ac.za/opencms/export/PUK/html/fakulteite/natuur/comp/hakruger_research4.pdf

[17] Information Security Forum, 2002.Effective Security Awareness Workshop Report .Electronic version found at https://www.igt.connectingforhealth.nhs.uk/Knowledgebase/Kb/ISF%20documents/Effective%20Security%20Awareness%2022-04-02.pdf

[18] Johnny, Mathisen.2004. Measuring Information Security Awareness – A Survey Showing the Norwegian way of doing it Gjovik University College.

[19] Jonathan Penn, Forrestor Research, 2009.Market Overview :IT Security in 2009 .
[20] Jonathan Penn,Forrestor Research ,2010 .The State of SMB IT Security and Emerging Trends: 2009 to 2010

[21] Luis Enrique Sanchez, Antonio Santos-OlmoParra& David G.Rosado, Mario Piattini, 2009.Managing Security and its Maturity in Small and Medium sized Enterprises. Electronic version of document found at http://www.jucs.org/jucs_15_15/managing_security_and_its/jucs_15_15_3038_3058_sanchez.pdf

[22] KPMG, 2006.Information security survey. Electronic version found at http://www.clubofamsterdam.com/contentarticles/27%20Electronic%20Identity/info

rmation%20security%20survey.pdf

[23] Mark Merkow& Jim Breithaupt, 2006. Information Security Principles and Practices by Pearson Education, Inc

[24] Mark Wilson (Ed.), Dorothea E. de Zafra, Sadie I. Pitcher, John D. Tressler, John B. Ippolito, April 1998.Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST Special Publication 800-16.Electrinic version found at *http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf*

[25] Mohammed ,Alnatheer, and Nelson, Karen, "Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context" (2009).Australian Information Security Management Conference. Paper 2.Electronic version found at http://ro.ecu.edu.au/ism/2

[26] NIST Special Publication 800-50, O2003.Building an Information Technology Security Awareness and Training Program. Electronic version found at http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[27] Norwegian Information Security Laboratory (NISlab) www.nislab.no

[28]Norsksenter for informasjonssikring (NorSIS) www.norsis.no

[29] Price Waterhouse Coopers,2010.The Global Maturity of Information Security Survey. Electronic Version found at http://download.pwc.com/ie/pubs/trial_by_fire.pdf

[30] Dzazali, Suhazimah, "Social Factors Influencing the Information Security Maturity of Malaysian Public Service Organization: An Empirical Analysis" (2006). ACIS 2006 Proceedings. Paper 103.Electronic version found at http://aisel.aisnet.org/acis2006/103

[31] The Maturity of SME IT Security Market and Emerging Trends: 2009 to 2010 by Jonathan Penn, Forrestor Research, 2010

[32] Thomas Schlienger and Stephanie Teufel, 2003.Information Security Culture-From Analysis to Change ,Information Security South Africa – Proceedings of ISSA 2003,3rd Annual Information Security South Africa Conference ,ISSA :183-185

[33] Institute of Electronic Governance, State Government of Andhra Pradesh http://www.ieg.gov.in/

9 Appendix

Questionnaire for Norwegian and Indian MSME's Survey

Starting Page for the Online Questionnaire

Thank you for participating in our survey on the subject of information security maturity. The survey consists of 26questions and takes approximately 10 minutes.

This study is conducted by Høgskolen i Gjøvik and Norwegian Information Security Laboratory.

All the 19 questions are related to information security in general, security awareness, culture, policies and spending in Indian Small and Medium Enterprises. To get a high quality response , it is important that you answer the questions honestly . Please read each statement carefully and select the right response that best fits your view and reality of your company. If the choice does not match your requirements, choose for a choice that closely matches you.

If you have any questions about this survey, Please do not hesitate to e-mail me at krishna@krimsh.com

Your personal E-mail address is kept strictly confidential. The data are evaluated in compliance with applicable privacy policy.

Thanks in Advance.
Best regards
PenmetsaMurali Krishna
Høgskolen i Gjøvik/Norwegian Information Security Laboratory (NISlab)

General Questions on Information Security

1. **What are the top priority information security goals for your organization?**

	Top priority	**4**	**3**	**2**	**Not at all priority**	**Don't know/does not apply**
Confidentiality						
Integrity						
Availability						
Traceability						

Managing Information Security:

2. **Which of the following best describes the information security structure of your organization?**

	Dedicated staff within the organization whose primary job function is information security
	Staff within the organization with a secondary job function of information security
	Dedicated individuals outside the organization whose primary job function is information security
	Outside experts through and outsourcing agreement
	None of the above
	I do not know

3. **Do you have any of the following in place to protect your computer and electronic data? Please indicate all that apply**

	Anti-virus software that is updated regularly
	Firewall
	Anti-spam filter
	Good password practices
	Process of regular back up of data

4. **Which of the following do you think are the greatest threat to your business information?**

	Greatest threat	**4**	**3**	**2**	**Not a threat**	**Don't know/does not apply**
Competitors						
Partners						
Employees, because they might intentionally or unintentionally leak information						
Employees using personal mail						
Employees using 3G devices						
Ex-employees						
Email without encryption						
Printing of information						
Industry espionage						
Outsourcing						
Malware (Viruses,worms,Trojans etc)						
Spam						

5. **Does your organization have a information security policy?**

	Yes
	No

6. Is the information security policy of the organization accessible to the employees via , for example , the intranet ?

	Partly
	Yes
	No
	No, but is planned

7. **What drives the creation of security policy for your organization?**

	Security breaches from external sources

	Improved business practices
	Auditing regulations
	Legislative regulations
	Protection of brand or image
	Security breaches from internal sources
	Industry standards

8. Is staff's knowledge about the information security policy or its guidelines measured ?

	Yes
	No

Security Culture:

9. Please rate the Information Security Culture of your organization?

	To a very high degree	**To a high degree**	**To some degree**	**To a low degree**	**Not at all**	**Don't know/Does not apply**
The employees of our organization are sufficiently aware of the information Security risks.						
The top management of our organization have enough information about IS risks						
The top management of our organization is convinced that IS is very important for achieving Business objectives.						

10. What are the top inhibiting factors for changing security culture in your organization ?

	Important Inhibitor	4	3	2	Not at all important inhibitor	Don't know/Does not apply
Insufficient Budget						
Employees Non seriousness						
Lack of right people to run the awareness activities in house						
Lack of management support						
Organization culture						
Fear and resistance to change from employees						

Security Awareness and Training Programs

11. Which of the following awareness campaigns are used in your organization to improve information security culture?

	To a very high degree	To a high degree	To some degree	To a low degree	Do not Plan	Don't know/Does not apply
Article in the newspaper						
Blogs						
Brochures and Flyers						
E-learning						
Film						

Newsletter						
Poster						
Security exhibitions						
Security quizzes and games						
Social Network						
Web portal						
Workshops for all employees						
Workshops for management						

12. How frequently does your organization organize information security awareness and training programs ?

	Every six months
	Once a year
	Every two years
	Less than every two years
	Every three years
	Do not do them at all
	I do not know

13. If so how ?

	Interviews
	Employee Survey by Questionnaire
	Observations and tours
	Audits
	None of the above
	I do not know

14. Which of the following elements do you think are covered in your organization'ssecurity awareness program? (Choose more than one option if appropriate)

	General information security awareness topics, but no training
	Review and agreement of compliance with current security policies and standards
	Direct and frequent updates/alerts on current threats to the organization
	Specific awareness activities or training sessions for high-risk user groups
	Measuring the effectiveness of IS awareness activities
	Incident reporting
	None of the above
	I do not know

15. Which of the following proportions of your company's IT budget is allocated for information security awareness ?

	Greater then 5 percent
	3 to 5 percent
	1 to 3 percent
	Less than 1 percent
	No separate budget
	I do not know

16. Do you plan to maintain or increase / decrease your information security awareness spending for the year 2010 to 2011 ?

	Increase more than 10%	**Increase 5 %- 10 %**	**Stay about thesame**	**Decrease 5%-10%**	**Decrease more than 10%**	**Don't know**
IS awareness programs and training sessions						

Demographic Questions

17. To which business sector do you belong ?

	IT
	Financial Services
	Pharmaceutical
	Government & Public Sector
	Other (please specify)

18. What is your position in the organization?

	Managing Director/Director
	General Manager
	Working in the Information Security Office
	Network and System Administrator
	Information Technology Executive
	Employee
	Other (please specify)

19. How many employees are working in your organization?

	1-19
	20-99
	100-250