knowledge platform

INFORMATION SECURITY: NURTURING A SECURITY CONSCIOUS WORKFORCE

A Knowledge Platform White Paper
April 2005

By Kanags Surendran
Director- Products and Solutions
Knowledge Platform

Knowledge Platform
19 China Street
#03-02 Far East Square
Singapore 049561
http://www.knowledgeplatform.com
+65 6236-7681

knowledge platform

Table of Contents

Introduction

Andy Grove's statement "Only the paranoid survive" seems to be apt when one considers the current state of affairs with regard to information security in most organizations. No matter how many security programs are installed in the network or on the desktop, unless the employee is aware of the security issues, there will continue to be lapses in security.
Quite often employees do not comply with the security policies of the organization. The non-compliance may be very insignificant, such as not taking regular backups or not ensuring regular updates of the anti-virus program settings. However, most managers can cite several cases of holdups in their departments due to loss of data or productive time caused by these very insignificant misses. The productivity loss is probably the least damaging of the outcomes of information security breaches. The situation is more dangerous when such errors cause a breach that might potentially open up the organization to deliberate and intensive threats from hackers and frauds. The worst case could be the loss of sensitive information that might lead to huge financial liabilities and losses, adversely affecting the reputation of the organization.

Considering the human factor as a key element in alleviating information security threats, this paper will present the business case for the need to invest in an information security awareness program to build/develop a security-conscious workforce. This document will also accentuate the advantages of using E-Learning for such a program.

Information Security threats

The information security threats today are more lethal than a decade back. For an organization to counter the threats, it must first define what it perceives as a threat for information and privacy.

In today's world, security threats can broadly be classified as internal threats and external threats. Internal threats primarily include accidental security breaches done by employees due to negligence or non-conformance and employee misconduct on systems. External threats, on the other hand, include virus threats, hacker attacks, and infrastructure failures such as fires, terror attacks, distributed denial of service attacks, fraud attacks and Spam.

While most organizations appear ready to face external threats, they are inadequately prepared for the threats that are likely to arise from within the organization. The internal factors are usually the most ignored when it comes to information security in an organization. External threats usually receive a lot of media attention and are well-known, which makes it easy for an

organization to focus on and eliminate the threat. The internal factors usually are not able to garner much media attention simply because they are suppressed. And unfortunately, some internal threats are not even detected.

As per the Ernst and Young Global Information Security Survey 2004, the Trojan horse and Internet worms were classified as the biggest threats. A close second was the threat associated with employee misconduct.

The Human Factor

The human factor in information security starts and ends with intentional or involuntary employee misconduct. The risks are compounded because of the fact that most often the concerned person uses unsophisticated methods to gain access to systems; Something as simple as an employee sharing his/her passwords or an old, disgruntled employee having access to the emails even after he has left the organization could cause a security breach.

The E&Y Information security survey 2004 findings indicate that most of the top ten incidents of loss of availability of critical business systems were due to internal causes. Of those who reported an outage due to a Trojan horse or Internet worm, 21% indicated that the origin of this virus was internal to the organization. 78% of the respondents attributed internal causes as reasons for software failures while 84% felt that internal causes again were responsible for employee misconduct.

An average employee does not know about the information security threats as he goes about doing his work. It is up to the organization to ensure that not only should the average employee be aware about these threats but also understand what needs to be done in case he/she notices a potential issue. Even though the senior management is aware of these information security threats, not much has been done to educate the other employees about them

Awareness, Governance and Regulations

The Information security readiness in an organization is not complete unless and until the human capital is bought in as a component. No amount of technology can protect an organization effectively if the human factor is ignored. It will only take one employee to open a virus=infected email from the Internet and initiate the spread of the virus in the organization's network. To ensure that the systems that are installed in an organization work to their fullest, it is essential that the users are educated and are made aware of the various security breaches and the ways in which these breaches can be prevented . It is equally important to educate the employee about the need to report suspicious activity and to act as per the company's security policy.

Information security should not be considered just as a component of the IT department but as a part of the Organization's Governance initiative. The cost associated with an information security breach is huge in terms of liability loss of reputation, loss of the customer's privacy, loss of productivity and loss of potential revenues. When the cost of security pitfalls is so high, it makes little sense for the senior management to ignore security concerns.

To provide effective security, organizations must know what they are trying to protect and from whom and who can be active participants in the exercise. This is the first step towards creating an organization-wide Information security policy. Some organizations have even gone a step ahead in creating a chief information security officer who is a part of the compliance department. The work does not end with the design and creation of a security policy but begins with it. The organization's defenses will be complete when it ensures that the employees are aware of the policies and practise them everyday.

This is where the Regulations have come in as a very good incentive for an organization. Regulations such as the Federal Information Security Management Act (FISMA), the Health insurance portability and accountability act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) in the USA require the government, health care industry and financial industry to provide for strict information protection and uphold privacy of information. These regulations also explicitly require the industry to provide training to their employees on such matters. As more regulations come into play, the chances of negligence would be higher too. In view of this, security awareness training is most likely to become mandatory in most industries in the next couple of years.

Security Awareness Program Requirement

Any Information Security Awareness program must help the organization in the following three ways:

1. Educate employees
2. Enforce policies
3. Expose suspicious activities

Educate Employees

It is not enough if the employee is given a booklet about security policies. The awareness program must help the average employee understand the need for security and help him practise caution when dealing with various aspects ranging from email to the Internet. The awareness program must help develop a new mindset in the employee - that of security awareness. The employee will also be required to understand the basics of security and what he/she can do to protect the information and privacy. Take the following case as an example:

While logging a problem, an employee of an organization grows suspicious on being asked for information about his password. He is aware that the IT administrator does not require this information to solve his problem. So, he does not comply with the request. His action prevents a breach of information security, which otherwise could have caused considerable damage..

Enforce Policies

Once the employee has the basic understanding of information security, he/she needs to understand the various security-related policies of the company and the reasons behind these policies. For example, if the privacy laws of the country indicate that one should not share confidential information about a particular client, the employee would refrain from discussing his client's information with his colleagues during the lunch hour.

Expose Suspicious Activities

The awareness program must also make the employees aware of the reporting requirements. To put an effective training into action, the employees must be made aware of what to do when they find out about a suspicious activity. Early identifcation of such activities would save an organization from an attack. Encouraging employees to report incidents without fear, ridicule or retributions is a must and this culture must be cultivated in the organization. For example, the organization could have an anonymous login, which could be utilized to pass on information if the employee feels threatened.

A complete awareness program would assist the organization in educating employees, enforcing policies and in exposing security threats.

Benefits of E-Learning

E-Learning is fast becoming one of the most preferred delivery methods for companies around the world due to its efficiency, effectiveness and economy. E-Learning, if used wisely, can help in driving an organization's security awareness program effectively. The primary advantages of E-Learning-based awareness programs are

- Economy – It is much cheaper than classroom training.
- Efficiency – It is convenient. It's anytime, any place 24X7 access and fast distribution makes the program less stringent. At the same time, ease of use, interactivity and game-based approaches make the learning experience fun and help increase retention.
- Effectiveness – Self-paced programs allow organizations to eliminate any disruption of operations making the returns on investment in these programs very attractive. The possibility of tracking students'

performances and other parameters ensure effectiveness of the program..

The appendix has a worksheet that calculates the costs associated with developing a security awareness program.

Information Security Awareness Program

The awareness programs can be structured in a variety of ways. The program aims to help employees in the organization to understand the security issue, drive home the need for committed vigilance and reporting.

Although an awareness program can be designed to address all constituencies in any organization, it is more effective when there is a focus on distinct groups. The organization can be classified under general employees and technologists. The target for the program will be those employees who use the IT systems, and those who handle corporate and customer information. This practically will cover almost 90% of the employees in any organization.

Information Security Course

The Information Security course is the core of the Information Security Awareness program. The entire course is about 1.5 hours long. It is divided into 5 modules of 15-20 minutes each and contains an assessment at the end. One of the best features of the program is its ability to drip-feed information to the user on a timed basis such that the participants are not overwhelmed. The entire course is structured around a simple, story-based instructional approach and is very interactive. The five modules are

1. IT Security: An Overview
2. Desktop Security
3. Security While Traveling
4. Email Security
5. Internet Security

The learning management system can be configured to send reminders to the users of their obligations and push the modules to them. The system can also generate customized reports to track the learner's stages and status.

Information Security Awareness Meter

The awareness meter consists of simple 10-minute assessments that are built in a game- based format. The user has to answer about 10 questions while playing a game. The scores are stored in the learning management system and reported to the manager if required. These assessments serve to reinforce the learning points and can be pushed to the employees at multiple time points

across a year to reinforce and gauge the level of security awareness in the organization. Knowledge Platform will be ready with a variety of such awareness games, which could be utilized on a regular basis to refresh the knowledge on information security in the workplace.

Customized E-Learning course

It is possible to customize the Information Security course to suit the additional requirements that your organization might have. The course can be adapted to include real life case studies and include any organization specific requirements.

Conclusion

Business Security Awareness training has become a critical part of an organization's information security directive. Although the need for such programs is recognized, most organizations often face issues with training. Either the organizations do not have enough budgets to cover classroom training, or they are not aware how E-Learning could be used effectively. In the worst case, organizations do not go in for training until it is too late.

E-Learning is being adopted across the world at a very fast pace and is an affordable and effective method to deliver an information security awareness program to a wide employee base.

Information Security Awareness Program Cost Analysis

Assumptions

1. The organization has 1000 employees
2. The turnover rate of employees is 10%
3. % of employees requiring awareness on Information security is 70%
4. The average monthly wages of an employee requiring training is $3500@ 22 days and 8 hours per day
5. There are no travel costs for the employees. i.e. the training happens in the same location as the employee's office
6. The average employee would require about 2 hours of one time classroom training.
7. Organisation has a SCORM Compliant LMS
8. The E-Learning course on Information Security will be 90 minutes and will be available over 12 months

Total Employees including contractors	1000
Turnover rate of employees	10%
% of employees requiring awareness of security	70%
The training department has invested in a Learning Management System	Y
Need an Annual Refresher Course/Assessment	Y

This analysis covers the expenses associated with the training and the opportunity cost of the employees stuck in class room training. The analysis also does not include the benefits accrued from the training such as improved productivity, nor does it include the detailed training required by IT professionals and IS department.

Training Options

Option 1: Classroom training

- The costs would include tuition, materials and infrastructure costs.
- Each training session can accommodate only about 40 persons and is for 2 hours duration. There can be up to 4 training sessions in a day.

Option 2: E-Learning – Custom development

- The organization owns a LMS and has an IT department to support the implementation
- The custom development costs include the cost of a subject matter expert
- The custom development costs include effort spent by the project management from the client side
- Approximate development cost of 25K for one hour of content

Option 3: E-Learning – Off the shelf product on asp basis

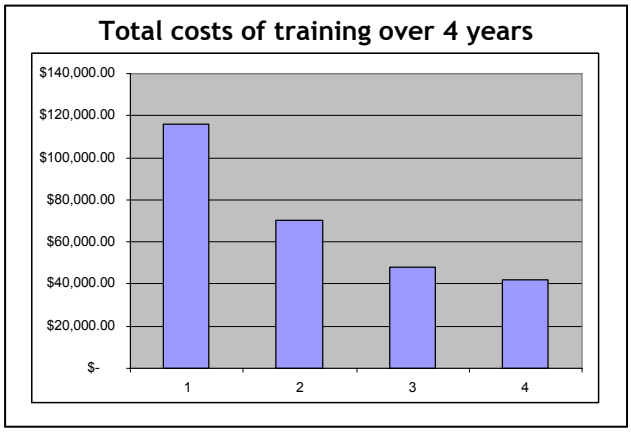
- Hosting fees for 12 months
- Product cost and subscription fees

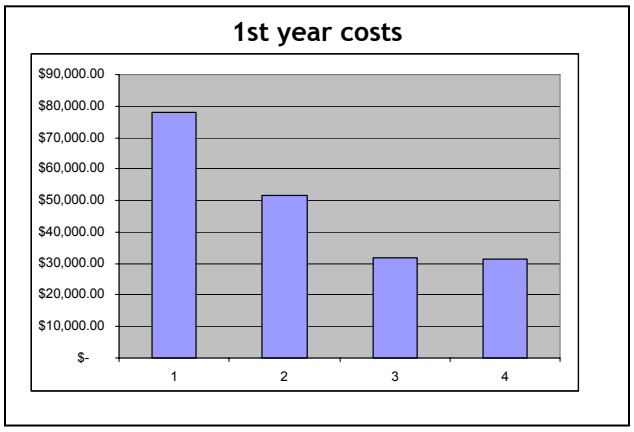
Option 4: E-Learning – Off the shelf product (enterprise license)

- Product cost
- Does not include internal cost of supporting the course which can be safely assumed at 20%

For more information on the training costs, you could download the cost analysis work sheet that can be found on our website. This spreadsheet also calculates a cost of a virus attack and the ROI of training in mitigating such attacks.

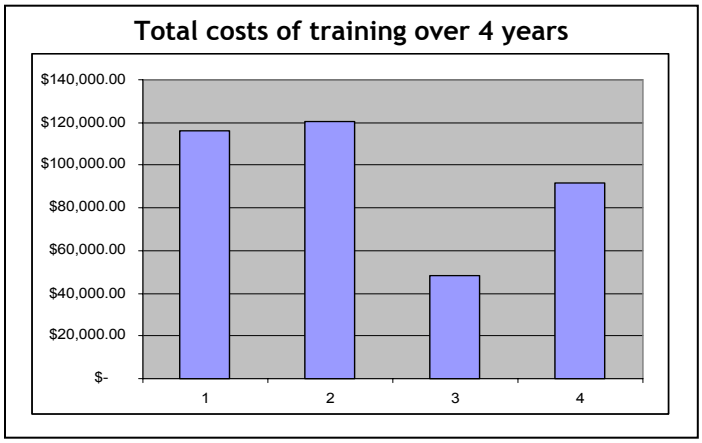
Training Solutions costs



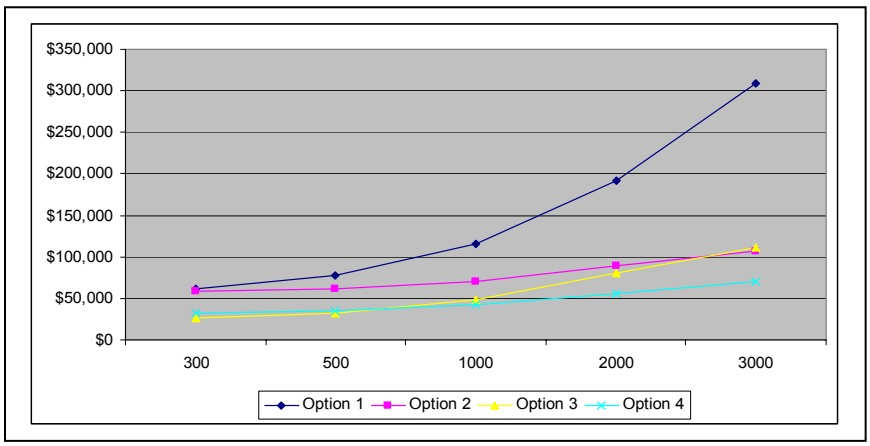


Sensitivity analysis

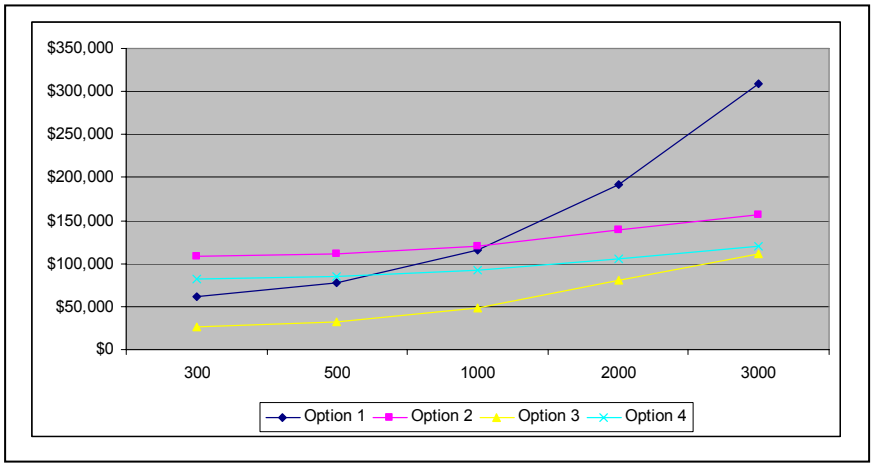
- Organization does not have a learning management system.



- Training costs at varying employee levels (assuming LMS existing)



- Training costs at varying employee levels (assuming LMS not existing)



As the sensitivity analysis shows, if the organization has employees ranging between 1 and 600 users, it is better to have the hosting done externally if the organization does not have a LMS. Irrespective of whether the organization has an LMS or not, increasing awareness of E-Learning is more cost effective.

About the Author

Kanags Surendran heads the products division for Knowledge Platform. Kanags has in-depth experience in IT requirements analysis, solution architecting and project management. Prior to Knowledge platform, as a Project Manager at Infosys Technologies Ltd, he has led multiple teams spread across various locations in India and the USA in helping clients to (a) develop technology roadmaps, implementation plans and strategies, (b) determine business requirements, (c) map business requirements to IT solutions, (d) conduct Gap analyses, (e) architect IT solutions, (f) define EAI architectures, (g) develop migration plans, (h) implement mission critical applications and (i) manage roll-outs and adoption processes. Kanags holds a MSc(tech) in Engineering Technology from BITS, Pilani, India (1997) and an MBA from INSEAD (2003).

About Knowledge Platform

Knowledge Platform is one of Asia-Pacific's leading instructional design, E-Learning content development and learning technology solutions companies. Established in early 2000, Knowledge Platform has offices in Singapore, Tokyo, Delhi and Islamabad. By providing services such as E-Learning Content, Instructional Design, Training Solutions, and E-Learning Technology Solutions, Knowledge Platform helps its clients to increase their learning efficiency.

Knowledge Platform has a rapidly growing, blue chip enterprise, banking, educational, and government sector client base.

The products division of Knowledge Platform specializes in creating generic and proprietary E-Learning products on subjects relating to business processes that enhance operations and reduce risk. The company has demonstrated leadership as a valued resource, subject matter expert and service provider in the areas of compliance including information security and privacy, code of conduct and anti-money laundering.

To learn how Knowledge Platform can help your company create a secure environment for maintaining information integrity, you could reach us at +65 6236 7685.