What Makes an Effective Information Security Policy?

Karin Höne and J.H.P. Eloff

It is a well-known fact that the information security policy is one of the most important controls needed within an organization to manage the implementation and ensure the effectiveness of information security. The information security policy is essentially the direction-giving document in an organization and defines the broad boundaries of information security. Furthermore, it indicates management's commitment to, and support for, information security in an organization and defines the role it has to play in reaching and supporting the organization's vision and mission.

Unfortunately, a common problem with most information security policies is that they fail to impact the users 'on the ground'. Documenting an information security policy that reflects the organization's vision and mission and at the same time entrenching the policy in the organization so that it becomes a normal and acceptable part of day-to-day operations is difficult at best. Quite often, users are ignorant of the policy's existence; users do not fully understand the document; it is too long or too technical; users do not see the relationship between the policy and their daily tasks and see it as a nuisance. In other words, the information security policy appears to be totally ineffective and is not achieving its aim of explaining the need and concepts of information security to the users.

What is an effective information security policy?

In the *Oxford Dictionary of Current English*, effectiveness is defined as "producing the desired results"[1]. In business terms, managerial success is measured against effectiveness, i.e. to achieve the organization's business objectives. Again, effectiveness is expressed in terms of achieving a certain result. Applying these definitions to an information security policy would thus mean that an effective information security policy assists in achieving the information security objectives of the organization. It is a fact that all businesses are becoming more reliant on knowledge and information to deliver value-added, quality services and to have a competitive advantage. Therefore, the protection of all information is becoming more important.

One of the main goals of an information security policy is to define the rights and responsibilities of information resource users [2]. An effective information security policy will help the users understand what acceptable and responsible behaviour is with regards to information resources to ensure the safe and secure handling of information in their daily tasks. In fact, to be fully effective the information security policy needs to incorporate both the users' needs for accurate and reliable information, as well as the business's needs for achieving its strategic objectives. In doing so, the users will be convinced that information security is not a necessary evil, but rather exists to ensure that the right information is available to them at the right time to make informed business decisions and achieve profit and success. In short, an effective information security policy is an understandable, meaningful, practical and inviting document that addresses the users directly and convinces them of the need for handling information resources securely.

What does an effective information security policy consist of?

Information security is becoming more and more a people and business issue and it is therefore imperative that the information security policy is adapted accordingly. At the end of the day, the users will determine how effective the information security policy really is. This means that the information security policy, and all supporting activities, should be completely user focussed — from the writing style and the way in which it is presented to the deployment of the document. The various supporting activities all have a role to play in ensuring the success and effectiveness of the information security policy and should therefore not be considered in isolation when creating the policy. This concept is illustrated in Figure 1.

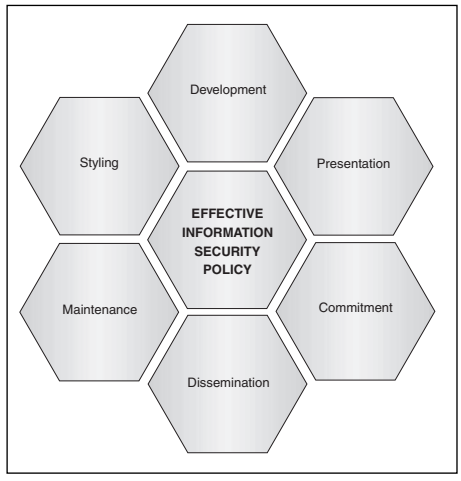

Figure 1: Supporting activities for an effective information security policy

The styling of the document, which describes the manner of writing, should at all times be consistent with the organization's overall communication style. It should in fact fit in with the organizational culture. This eliminates the risk of alienating the documenting from the rest of the organization's official documents and thus turning information security into an unfamiliar and foreign concept. The style and tone should furthermore be user-friendly and clear to ensure that the users understand the concepts surrounding information security [3] Using copies of other organization's information security policies or even samples found in the public domain, such as the Internet, can easily lead to creating a mismatched

document that users cannot relate to. Whereas smaller organizations tend to cultivate a culture of trust and reliance on user discretion, larger organizations often need stricter controls for proper management of the more diverse environment. The organizational approach needs to be reflected in the style of the information security policy, which cannot be easily done when creating a 'cut and paste' version. Very often, the information security policy is turned into a highly technical document crammed with as much detail as possible, thus making it cumbersome and difficult to understand. For a non-technical person the document then means little and the user cannot relate to what is expected acceptable behaviour. Unfortunately, it is also true that the documenting of the information security policy is often left to the technical staff, who admittedly may know the information security technologies very well. The same technical staff have, however, little or no understanding of their users and how information security should fit into the broader organizational culture. This problem can be eliminated by ensuring that the information security policy is developed in conjunction with representatives of all the stakeholders who have a vested interest in the policy's success. Even though this takes up more time and resources initially, this approach can go a long way towards ensuring that the information security policy is accepted and therefore is an effective control measure [4]. The actual wording of principle statements is also critical to the effectiveness of the information security policy, as a misinterpreted statement can damage an organization's information security arrangements.

Presenting the document as a fun and attractive communication will ensure that the users take note of it and the messages it contains. This also implies that the document should not be long, but rather short, concise and to the point. The main document should rather be very brief, but with interesting cartoons or dialogue which the users can relate to. Supplementary policies, standards and guidelines should then be developed to support the main policy and detail the specific topics. The document should, however, at all times be presented as a quality deliverable to help underline the fact that information security is important and that the organization is not adverse to taking it seriously and treating it as a business-critical issue.

The commitment and buy-in from top management is vital for the effectiveness of the information security policy, as people generally live by example. Changing the attitudes and the behaviour of users starts right at the top with the chief executive officer (CEO) and the executive committee [5]. Users will not believe in the information security policy if they do not see their leaders conforming to, and living by, it. In fact, for the policy to be truly effective, it needs buy-in from all levels of the organization.

An information security policy cannot be effective if the users do not know about it. Therefore, it is important that the information security policy is correctly and appropriately deployed throughout the organization and actually brought to the users. There are various methods that can be used to disseminate an information security policy. The dissemination can be done through distributing full paper-based or electronic copies of the document, through publishing the document on an internal communication site such as the intranet, through summarizing the policy on colourful brochures. Once again, the dissemination method should ideally fit in with the organization's traditional dissemination methods. This does not mean that there is no scope for creativity, but rather that there will be certain dissemination methods that are easier to implement and more acceptable to the organization than others. In fact, a clever marketing-type drive will ensure that the users take definite note of the policy and are more likely to understand and adhere to it. The information security policy can also be deployed during an awareness session, which gives the opportunity to reinforce and explain the message of the policy immediately to the users. An advantage of using this method can furthermore be that top management support can be visibly demonstrated. The fact that top management is willing to take the time to attend an awareness session sends a far stronger message regarding their support for information security than a signature on a document [4].

The information security policy should be a living document. It should at all times grow and develop with the organization to ensure that it supports the achievement of the organization's vision and mission. Updating the information security policy regularly has several advantages. These include keeping in touch with the organizational developments and ensuring that the document does not become static and outdated [6]. As a review of a high-level policy document often introduces changes to the organization, the review period should preferably fit in with the organization's normal business cycles. During certain times in the cycle, the users will be more acceptable to change and the re-enforcement of ideas and principles, than at others. Financial year-end periods are for example critical and busy periods and the users do not want to be exposed to new ideas or changes at such times.

To achieve an effective information security policy, it is important that the various supporting activities are considered and implemented with care. These supporting activities help as a whole to create an effective information security policy.

Conclusion

An effective information security policy is a policy with which the users can identify and from which they can clearly see what is expected from them in terms of handling information resources. The effectiveness of the policy does not so much rely on the right content, but rather the way in which the content is addressed in the document and ultimately communicated to the users. At the end of the day, an effective information security policy, will directly result in effective information security.

Karin Höne Department of Computer Science, Rand Afrikaans University, KarinH@gensec.com

J.H.P. Eloff, Department Computer Science, University of Pretoria, South Africa, eloffrkw. rau.ac.za

References

[1] *Oxford Dictionary of Current English.* Oxford University Press,1998.ISBN 0-19-860233-2.

[2] Sholtz, Paul, 2001. Internal Security Rules and Risks. http://www.newarchtectmag.com/archives/2001/07/sholtz

[3]PricewaterhouseCoopers, ITP.net. August 2001. IT Security Survey: Issues and Trends in the Middle East. http://www.itp.net/survey/security.htm

[4]Human Firewall Organization.2002. Human Firewall — Issues.http://www.humanfirewall.org/issues.htm

[5] The Software Engineering Institute (SEI), Carnegie Mellon University. May 2002. State of Practice of Intrusion Detection Technologies, http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99028chap04.html

[6] Briney, A. September 2000. Security Focused.http://www.infosecuritymag.com/2000survey.pdf

E-COMMERCE: THE DARK SIDE

Card Fraud — More Serious Than Given Credit For

Bill Boni

There is a war going on in cyberspace and the 'good guys' appear to be losing it. The combat is not just cyber terrorists probing and defacing military, political or economic targets, but much more commonly at this point, between cyber criminals and managers of IT staffs supporting E-commerce operations. The facts are that a class of 'elite' hackers is now commonly able to attack sites, extract credit card account information then cover their tracks by destroying digital evidence along their path. These intruders have become more brazen as they have become more successful.

The situation has got so dire that Gartner, a leading consulting organization, estimates that cyber-fraud cost companies over $700 million in 2001. The Gartner study claims that over 5% of online shoppers have experienced credit card fraud and nearly 2% suffered identity theft. These numbers are staggering and put into perspective the often-quoted comments from credit card companies that online fraud is a tiny percentage of total charges. Of course they are tiny when compared with the vast amount of total credit card purchases. But to say that fraud against one buyer out of 20 is immaterial when they have suffered from cyber-fraud is disingenuous at best, misleading at worst. It is not the dollar value of the losses at present that constitute the problem; it is the fact that so many of the online shoppers are defrauded in some manner. Imagine for a moment what would have happened to credit card use in general if 5% of the users had fraud committed against them! It's pretty obvious that many, perhaps most people would simply decline to use credit cards.

The collective impact of such losses is probably one reason why E-commerce has lagged behind the dizzying rate anticipated by its advocates. There are too many people who have been victimized to ignore. If the consumer experience of cybercrime is bad the corporate counterpart is at least as bad. The police and law enforcement agencies have had some successes, but largely against the less skillful and less successful criminals. Reviewing the list of unsolved high profile cybercrimes, one is struck by the fact that the list continues to grow, and none of the more serious crimes have been solved.

For example, in November 2001 an attacker extracted a number of customer accounts from the Playboy.com site. The intruder actually showed customers he/she had successfully penetrated their accounts by sending them their credit card numbers via email.

One of the most disturbing cases happened in the summer of 2001when a hacker managed to obtain personal information of as many as 350 000 customers of Ecount, a gift certificate company. The criminals attempted to extort $45 000 or they threatened to release the information. The investigation has been open now for nearly a year with no successful resolution. In fact the criminals have taunted managers at Ecount for their inept investigations and inability to find them

We have previously discussed the CD Universe case, which dates from January 2000. In one of the most successful attacks ever, about 350 000 credit card numbers were taken from the company's website. 'Maxus', as the criminal identified himself or herself, is still at large and although many suspect the criminals are connected to Russian organized crime there has been no arrest so no closure.

The fact is that law enforcement agencies of leading countries simply have not been able to bring to justice hackers who perpetrate these attacks. Although police officials are getting better at tracking and