Cultivating an Atmosphere of Proactive Computer Security to Mitigate Limited End-User Awareness

M. Styles[1] and T. Tryfonas[2]

[1]IMServ Europe Ltd
[2]Information Security Research Group, Faculty of Advanced Technology,
University of Glamorgan, Wales, UK
e-mail: ttryfona@glam.ac.uk

Abstract

It is becoming increasingly important that employees are taken through a more rigorous security-awareness training programme, in order to protect their personal computer and the networks behind it and to 'protect them from themselves'. Virus and spam writers have begun to try to fool employees with 'social engineering' techniques, which prey on an employee's willingness to believe in an email sender-name or inquisitiveness stirred by the email subject title. The purpose of this case study paper is to demonstrate that, no matter how complex computer security systems are, effort should be concentrated and focused on employees to improve their security awareness. Each employee needs to become a 'Security Deputy' to the company's computer security staff and he or she needs to take some responsibility for preventing security breaches – whether inside the workplace or not. In this paper we investigate whether it is possible to remove the ability of users to compromise computer security. As it is easy to unwittingly spread a virus, or open security vulnerabilities, should users be held responsible for their actions? Such actions might damage a company's systems perhaps even more than malicious employees, through simple ignorance of security issues. Later in this work we explore the options available to increase the security awareness to a higher level, including automating security policy enforcement that will be examined as a method of removing the 'human element'.

Keywords

Security management, Awareness, Human Element, Policy Automation

1. Introduction – The Different Threat from Within

This paper presents a case study based on a real organisational project that aimed to establish whether it was possible to cultivate an atmosphere of proactive computer security amongst employees whose job does not generally require computer expertise. The main aim was to demonstrate that, no matter how robust computer security systems are, a significant amount of effort should be concentrated and focused on employees, in order to improve their security awareness. In today's complex and interconnected business environment, each employee should be required to become a 'Security Deputy' and take responsibility for preventing security breaches, whether inside the workplace or not.

Each employee is unwittingly duty-bound to consider the security of his or her own computer, as well as the security of the company servers and networks simply by operating and interacting with his or her personal computer and the applications which it runs. Few people even realise that the simple act of opening what purports to be a joke email, but in fact turns out to be a virus-infected email, can cost a company thousands of pounds in lost revenue. Spam writers routinely target poorly protected PCs to act as email proxies and generate huge amounts of email traffic, which slows down networks and waste time of the recipients. If a malicious insider represents a form of the threat from within, limited user awareness is another potential kind of internal threat.

User involvement in security awareness is not a new initiative (e.g. Wilson & Hash, 2003; Furnell & Phyo, 2003), but lately the security community encourages security officers to concentrate on security awareness initiatives, instead of investing in the latest 'new security gadget'. Barrett (2006) for example, claims that by training the people well, knowing what the risks are, an organisation reduces the need for the latest security products. The strength of organisational cyber-defence is with knowledgable workforce. It is becoming clear that organisations need to focus as much on user involvement in security, as they do in implementing a new firewall or anti-spyware device.

Bejtlich (2006) has suggested that the aim for network security is not a 'totally secure' network, but one which is as 'secure as possible', by striving for what he terms a 'defensible network'. He places particular emphasis on activities such as monitoring and control, all of which involve a strong human element. In his book 'Beyond Fear' Schneier (2006) evaluates security and attempts to demystify it in a plain-talking manner. Security 'trade-offs' must occur he says, as we make security trade-offs between implementing draconian security systems and enabling business to be conducted with ease.

The goal of the present paper is to present our initiative, including in detail: a detailed description of the method adopted (section 2), the security tests performed and their results (section 3), a discussion on the project's success factors (section 4) and finally our concluding remarks (section 5).

2. Selected Case Study and Research Method

Our experiments were undertaken in a medium-sized company including both technical and non-technical staff. Questionnaires were designed to gauge employee security awareness and a subsequent campaign was launched to educate employees in security issues. Efforts were made to involve users in addressing areas in which security was lacking and employees were encouraged to participate in establishing a more secure working environment. The results were very positive and a marked improvement in security awareness was measured. Even employees who had relatively low computer competences felt that they were becoming active participants in securing the business.

The project methodology was based on a series of exercises, which were designed first to gauge the general level of security awareness and then to raise employee competence towards establishing a proactive security environment. Ideas on questionnaire design were sought from a number of sources that included good practice guides in questionnaire design (e.g. Burgess, 2001). We formulated a set of questions and then assigned them to an external survey company to administer the survey, after a number of different Internet-based solutions were taken into consideration as alternative approaches.

The project was conducted under the following general sequence of tasks:

1. Initial security awareness experiments. Those included surveys and social engineering tests.
2. Research into previous work on methods for enhancing security awareness. A number of authors have discussed ways in which security might be improved by tackling the relative lack of security knowledge of most company employees.
3. Analysis of options for improving security awareness. Security campaigns based on posters and emails were considered in further detail.
4. Security awareness training sessions – initiating a program of security training amongst staff.
5. Analysis of options for removing user interaction to improve security
6. Analysis of alternatives to the relatively 'open' systems that employees currently enjoy: Is it possible to remove all internet/intranet and email access?
7. Second phase security awareness experiments ('identification of phising' test).
8. Evaluation of the project and the research based on the outcome of the second phase against the results of the initial testing. How successful have the methods employed in the study been in improving employee security awareness? Are users now routinely practising a proactive and preventative computer security policy? Tests were conducted on the employees to compare their attitudes to security matters.

Regular meetings were held with employees to help gauge the effectiveness of any improvements in security awareness.

3. Security Tests and Analysis of Results

A number of exercises were performed on staff at the target company to gauge security awareness and attitudes towards improving security within the organisation. A series of password cracks were performed to understand the patterns that people had in choosing monthly passwords and offenders who regularly chose insecure passwords were targeted for further testing. A report from the cracking software, l0phtCrack, clearly showed that 61.49% of all passwords surveyed were deemed to be "*High Risk*". It was established that many company employees used simple dictionary words and obviously did not consider the password strength when

selecting a new password. The great majority of network passwords were cracked in less than one minute, with many taking just a few seconds processing.

Following the password crack exercise two questionnaires were designed, an 'Information Security Survey' and 'Email Scam Test'. These instruments were sent to all employees to gauge user reaction to requests soliciting information. Invitations were sent to company employees automatically via an external Internet services company. The first questionnaire was a general security survey containing 43 questions relating to information security issues and the second was a short test of employees' skills in identifying a specific security threat – in this case email fraud attempts known commonly as 'phishing'. Phishing can be a threat to both the individual and the company, with 'spear phishing' targeting a specific company or group of individuals. The Email Scam test was based on genuine emails that had been received by the organisation.

Of the 133 employees invited to complete the survey, 114 started the survey and 102 completed the survey.

Key statistics obtained from the security awareness questionnaire:

1. 100% use Instant Messaging (IM) such as MSN Messenger – surprising because IM should be prevented by the corporate firewalls. This illustrates how IP port-morphing IM applications can circumvent traditional security measures.
2. 98% are aware of a firewall's purpose – most users have home PCs which have personal firewalls.
3. 95% surf the Internet every day – browsing the Internet is now part of the daily ritual of modern life.
4. 100% believe information security is necessary – an encouraging statistic!
5. 73% believe their password is difficult to guess – this was a worrying figure because it is completely erroneous. It is based on the employees' incorrect assumption that using an unusual dictionary word or place name, with the addition of extra characters at the end, constitutes a strong password.
6. 15 users admitted to sharing passwords – it is an unfortunate fact of business life that employees will share user accounts and passwords if it enables them to complete the objectives set by management.
7. 44 users believe common dictionary words are valid passwords.
8. 34% have written down complex passwords at some time.
9. 41 users (approximately 25% of all employees) have utilised USB memory devices to copy files off-site.
10. 98% know that encryption is a technique for scrambling data but only 12% have ever encrypted files or email. Encryption is not generally used within this company, although this is changing.
11. 38% do not understand that email can be intercepted in transit.
12. 25% have accessed company resources over a home or public wireless connection.
13. 33% have transported confidential documents on a laptop or PDA.

14. Most users believed that common social engineering attempts may be rebuffed by most users – although in practice this is unlikely to be the case as demonstrated by many social engineers (Mitnick & Simon, 2002).
15. Many users have tailgated cars into the car park or into the building because of a forgotten access card – demonstrating the ease with which a social engineer could enter the building.

16. 28% have challenged an unaccompanied visitor.

Key statistics obtained from the email scam test:

1. 87% could recognise a Nigerian 419 phishing email.
2. 86% recognised an oil shares price scam.
3. 19% could not recognise a fake PayPal request for account information.
4. 23% could not recognise a false Lloyds bank account request.
5. 16% could not recognise a false MSN account request.

Expansion of the project to a larger corporate audience began in early 2006 when the author was appointed to manage a review of IT security across the group of companies (approx. 40,000 employees total) and to lead the subsequent creation of a team of 'security champions' throughout the organisation. A Computer Based Training package was designed to improve user security awareness and was sent to 21,000 global computer users in 9 languages.

4. Success Factors for End-user Security Engagement

Options for removing user access to the Internet were evaluated. However, modern businesses rely on the Internet. A massive amount of inter-company communication is facilitated through Internet technology, such as email, Instant Messaging, Voice over IP, HTTP and FTP file transfers and web browsing. The Internet is an integral part of most people's lives, both at work and at home, and to remove access to it would severely limit the business functionality. Given this reliance on Internet connectivity, is it conceivable that user access to the Internet should be removed in order that the company in question should feel more secure? It was concluded that it is not practical to severely restrict user access to Internet resources since the company's business depends upon it.

A series of campaigns were therefore embarked upon in order to improve user security awareness in the company. A 'lunch and learn' session was arranged for the company Board and IT security was explained with a questions and answers session afterwards during lunch. User induction training for new employees was enhanced with a section on IT security which attempted to educate them about the risks that the company faced every day - from attempts to gain access through the company firewalls (average 500,000 attempts per day via automated/hacker port scans etc.), to the sheer volume of email spam/viruses processed by the company email firewalls.

Feedback from the security surveys and information security emails was very positive because users could relate to the topics covered since most people nowadays have experience of home computer systems which are affected by the same security issues such as email spam, phishing and viruses. Users found that they could apply the same principles at home as they could at work and achieve similar results; namely, a reduction in the number of security incidents.

At a corporate level, the formal incident notification process throughout the group of companies began to help manage security incidents in a coherent manner across the disparate group of companies. This approach to IT security marked a distinct change in attitude for the parent organisation which had previously held a view of security as merely an in-built component architecture of deployed IT systems which would magically 'take care of itself'. It was demonstrated at a number of meetings that information security is a continuous process and not a 'silver bullet'. Information security needs senior management buy-in and sponsorship, otherwise departments will find it too easy to ignore and may expose the company to significant risk.

In the success of this end-user engagement initiative, a number of factors therefore were perceived to be of vital importance. In summary those were

- **Externalising the exposure:** tests such as password analysis were useful in order to make users to revisit their assumptions about 'strong' passwords and operational security and also demonstrated to senior management the real level of threat. In turn this facilitated the second factor, following.
- **Engagement of the senior management:** the education process started from the top. In this respect it demonstrated to all members of staff that the company was serious about safeguarding information security and sat a good example.
- **Assessment based on an on-line survey medium:** an on-line questionnaire made it easier for staff to fill in and engage into the learning process by good numbers. In addition the hypermedia presentation of questions and answers facilitated the end user understanding as opposed to a dry paper-based exercise.
- **Tests and demonstration materials drawn upon real incident data:** the employees experienced through those tests realistic situations, as those were built on data collected within the company's computer security systems (e.g. received phising and scam emails, spam and malware etc.). This created a realistic environment for tests and users could relate the test questions to their everyday experience.
- **Embedding an IT security component in new starters induction:** much neglected by many companies, raising awareness on day zero was assessed as a very positive measure, as staff at all levels go through a process that initiates or reinforces their expectations of security in a digital world.

5. Conclusions

This project was executed during late 2005 and most of 2006, during which time a number of terrorist incidents occurred both internationally and within the United Kingdom. Given this context of heightened security requirements within our social life, it is reasonable to expect that company employees will begin to scrutinise their own behaviour, and indeed that of their colleagues. So this project is timely, as users will be much more willing to undertake reasonable information security precautions. However, information security is considered a 'dry' subject as far as most users are concerned and care must be taken to avoid users becoming complacent due to information overload.

Corporations are beginning to realise that information security must be extended to capture the 'hearts and minds' of employees, if maximum protection of company assets is to be achieved. Technical solutions are not enough. The results of the experiments undertaken by company employees throughout the course of this research case show that with good education, and then good practice, that it is possible to improve the security of the working environment.

Company employees demonstrated improvement in security awareness, following their involvement in the exercises and awareness training. Users were made explicitly aware of the realities of IT security with pertinent questions asked in order to force them evaluate their own reactions to a situation which may escalate into a security incident. For example, the illustrative questionnaires helped many people to realise that they have the potential to place the organisation at risk through their actions when handling email attachments. They have subsequently changed behaviour and sought to question their responses to potentially damaging situations as they may arise during their regular work with email.

Another example is with the password analysis, as their results were very useful in demonstrating the weakness of poor password selection. The subsequent advice offered to employees on ways to improve password strength was well received and acted upon. Most employees commented that they were surprised to see those compromised in a short amount of time and that it was now a lot clearer that a poor password selected for its convenience represents a security risk.

In the past, security had almost seemed to be a 'dirty word' and was not considered worthy of special emphasis, but now it was beginning to be seen as an essential element of business life. Many times security was mentioned when discussing the implementation of new systems, when previously it would not have even been considered. Our initiative was successful in improving the attitude of many employees, and the notion of an on-going requirement for information security within the target company and the corporate parent company was recognised as a direct result of the work undertaken. The group of companies that participated in this project were predominantly engineering and electronics industry businesses, i.e. companies which generally lagged behind in the adoption of cutting edge computing-related technology. However, the advances made in improving security awareness at

the target company have had a great influence on the parent corporation and significant improvements in overall information security have happened as a result. The positive security culture now experienced by the target company would not have been possible without running this project.

References

Bejtlich, R. (2006), Addison Wesley, *Extrusion Detection: Security Monitoring for Internal Intrusions*, ISBN 0-321-34996-2

Barrett, N. (2006), *Staff form strongest line of defence*, IT Week Magazine 27th March 2006, p16

Burgess, T. F. (2001), University of Leeds *"Guide to the Design of Questionnaires"* [on-line].

Furnell, S. and A. H. Phyo (2003), "Considering the Problem of Insider IT Misuse", *Australian Journal of Information Systems*, 10(2): 134-138.

Mitnick, K. and Simon, W. (2002), Wiley Publishing Inc. *The Art of Deception.* ISBN 0-471-23712-4.

Schneier, B. (2006), Wiley Computer Publishing, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, ISBN 0-3870-2620-7.

Wilson, M. and Hash, J. (2003), "Building an Information Technology Security Awareness and Training Program", NIST Special Publication 800-50.