E-MAIL SECURITY AWARENESS AT NELSON MANDELA METROPOLITAN UNIVERSITY (REGISTRAR'S DIVISION)

Ryno Boshoff[1], Johan van Niekerk[2]

[1]Nelson Mandela Metropolitan University
South Africa
[2]Nelson Mandela Metropolitan University
South Africa

ryno.boshoff@nmmu.ac.za[1], johanvn@nmmu.ac.za[2]

ABSTRACT

Electronic mail (e-mail) has become a critical business tool within most modern organisations. The proper security features need to be in place to ensure confidentiality, integrity and availability of business related information. After the security features are in place, all staff members need to be educated in the proper use of these features and the proper use of confidential information (ISO SANS 17799, 2005).

This paper presents a survey that was performed in the Registrar's Division at the Nelson Mandela Metropolitan University (NMMU). Structured interview questions were compiled by the researcher. The interviews were conducted on a one-on-one basis with the interviewee. The findings were documented and recommendations were made to improve the usage of the e-mail system and the awareness of security issues amongst the staff at NMMU (Olivier, 2004).

KEY WORDS

NMMU, E-mail, Awareness, Policy, Passwords

E-MAIL SECURITY AWARENESS AT NELSON MANDELA METROPOLITAN UNIVERSITY (REGISTRAR'S DIVISION)

1 INTRODUCTION

E-mail has evolved into a critical business tool in almost all modern organisations. It is not uncommon for an organisation to use an e-mail system as its primary communication method. The information sent and received via e-mail is often of a sensitive and/or confidential nature and should be properly secured (Cisco Networking Academy, 2005).

Although easy to understand and use, e-mail is not a perfectly secure communication medium. In order to protect the contents of an e-mail, organisations should ensure that the necessary security features are in place. Having these security features in place still does not guarantee the security of the information. It is also necessary to educate the end users about these features and about the methods that unauthorized persons may use to get access to the organisation's information. This will help with the detection and prevention of threats and unwanted attempts to access any business information and will ensure confidentiality, integrity and availability of the organisation's information (Cisco Networking Academy, 2005).

The Nelson Mandela Metropolitan University (NMMU) has a link on its staff portal to a website that was designed and is maintained by NMMU, dedicated to communicate Information Security awareness amongst NMMU staff. The purpose of this website is to make the latest Information Security information available to staff at the NMMU and to communicate the latest Information Security (IS) information. This website also has links to the NMMU E-mail Policy, the NMMU Information Security Policy and, guidelines and tutorials with some Information Security fundamentals that have been developed for computer users at the NMMU. Every person using a computer within the NMMU is supposed to go through this basic information. These guidelines and tutorials aim to ensure confident, motivated and educated staff able to

secure business related information. Unfortunately very little or no information exists to verify that these guidelines and tutorials actually work.

This paper aims to help address this lack of knowledge. The paper presents the results of a survey done at the Nelson Mandela Metropolitan University in the Registrar's Division to determine the level of awareness concerning e-mail security amongst end users.

2 RESEARCH DESIGN AND METHODOLOGY

A qualitative approach via interview schedules was used to obtain the data. The researcher's aim was to gain an in-depth understanding of the awareness of the staff on e-mail security and their attitude towards the protection of business related information. Closed, fixed-response interviews were used and interviewees were all asked the same questions. They were then asked to choose answers from among the same set of alternatives (Kvale, 1996).

The study was done at NMMU in the Registrar's Division. The sample consisted of 30 staff members, 5 from each department. The Registrar's Division has a total population of 99 staff member. The researcher chose to do the study in this division due to the availability to all staff during office hours. The aim of the study was exploratory and descriptive. The survey questions were created after an extensive literature study during which the researcher attempted to establish the level of e-mail security awareness in the NMMU Registrar's Division (Olivier, 2004).

Due care was taken to ensure respondents participated voluntarily and the entire study was done with full ethical clearance from the relevant authorities (Kvale, 1996).

3 SURVEY RESULTS

3.1 Direct questions

Question	Yes	No

1	Do you know whether there is an E-mail Policy at NMMU?	20	10
2	Have you read this E-mail Policy?	10	**20**
3	Do you open e-mails from unknown people/sources?	**22**	8
4	Do you have a disclaimer in your new e-mails?	5	**25**
5	Do you use your work e-mail account for personal e-mails?	**28**	2
6	When using your work e-mail account for personal e-mail, do you make it clear that these e-mails are an expression of your personal views and not those of the University?	8	**20**
7	Do you use the university staff and student distribution lists for non-university business?	0	30
8	Do you make use of encryption in the e-mails you send?	4	**26**
9	Do you make use of digital signatures in the e-mails you send?	4	**26**
10	Do you access your work e-mail account from your mobile phone or laptop?	0	30
11	If you do access your work e-mail account from your mobile device or laptop, do you know the risks associated when doing this?	0	0

12	If you do access your work e-mail account from your mobile device or laptop, do you know the counter measures to ensure proper security is kept?	0	0
13	Do you access your work e-mail account from home?	8	22
14	If you do access your work e-mail accounts from home, do you know the risks associated when doing this?	0	**8**
15	If you do access your work e-mail accounts from home, do you know the counter measures to ensure proper security is kept?	0	**8**
16	Have you given your username/password to Information and Communication Technology (NMMU ICT) staff?	**14**	16
17	Is there somebody that knows your password?	**17**	13
18	Is your password written down anywhere so you will not forget it?	3	27
19	Do you have a password protected screensaver?	4	**26**
20	Do you use the same password in more than one account?	7	23
21	Does your password consist of special characters?	0	**30**
22	Does your password consist of uppercase and lowercase characters combined?	13	**17**
23	Does your password consist of more than 6 characters?	28	2

24	Does your password consist of numbers and characters combined?	6	**24**

Question		**0 people**	**1 person**	**2 people**	**3 people**
25	How many people know your password?	13	**11**	4	2

Question		**0-5**	**6-10**	**10-15**	**16-20**	**>21**
26	How many new e-mails do you send a day?	7	**10**	6	4	3
27	How many e-mails do you forward a day?	2	**16**	8	4	0
28	How many e-mails do you receive a day?	0	2	**15**	9	4

Question		**0-20**	**20-40**	**40-60**	**60-80**	**80-100**
29	What percentage of the e-mails sent and received do you consider as confidential?	1	**12**	8	8	1

Question		Never	When forced	3 Months	6 Months	12 Months
30	How often do you change your password?	**12**	**17**	0	1	0

Question		Yes	No	Do not know
31	Do you have a Virus Scanner installed on the work PC?	7	0	**23**
32	Does your Virus Scanner scan incoming/outgoing e-mails?	0	0	**30**
33	Is your Virus Scanner updated regularly?	7	0	**23**

Question		No Screensaver	5 minutes	10 minutes
34	If you have a password protected screensaver, after how many minutes does it become active?	**26**	3	1

3.2 Specifying questions

35. Do you have any comments concerning the NMMU E-mail Policy?

Twenty staff members have not read the policy so they had nothing to say about the policy. Two of the staff members said it is a good E-mail Policy and the other eight said it is easy to understand and to implement.

36. What do you do with e-mail that you open from unknown sources?

Eight staff members said that they always delete the e-mails received. Ten staff members said that they have to process e-mails received from unknown people or sources. They receive requests for information on students or staff members that have to be processed and routed to the appropriate person. Twelve staff members confirmed that they open e-mails from unknown people or sources out of curiosity.

37. Do you know why a disclaimer is needed?

Twenty three staff members stated that they did not know why a disclaimer is needed. Four staff members said it was to help protect NMMU against any legal actions that could be taken against them because of an e-mail sent. Three staff members said it was the same as a signature within an e-mail.

38. When using your work e-mail account for personal e-mail, how do you make it clear that these e-mails are an expression of your personal views and not those of the university?

Five staff members stated that they use a disclaimer in the signature to protect them against legal action. Two staff members said they do not mention NMMU in any way in the personal e-mails they send, so the person receiving the e-mail will know it is not an expression of NMMU. One staff member said that he/she states it in every e-mail that is sent by that staff member.

39. Do you know why it is good practice not to use you work e-mail account for personal reasons?

Thirteen staff members said they did not know why it is good practice not to use a work e-mail account for personal reasons. Ten said that they were paid a monthly salary to work, no personal e-mail should be allowed. Six

staff members said that you could receive and forward viruses that could damage, destroy or deny services, and three staff members said his/her e-mail account was the property of the NMMU and should be used according to the rules and regulations stated by NMMU.

40. What do you consider as confidential?

Nineteen staff members who were interviewed considered their personal e-mails to be confidential. Thirteen staff members considered student and staff information in e-mails to be confidential. Ten staff members considered work related e-mails to be confidential. Five staff members considered financial information in e-mails to be confidential. Three staff members considered legal information in e-mails to be confidential.

41. With regards to question number 8 regarding encryption, if you indicated that you do not make use of encryption; can you please elaborate why not?

Twenty four staff members did not know how to activate and use encryption in the e-mails. Two staff members did not see a reason why encrypting their e-mails was important because they did not consider their e-mails to be confidential.

42. With regards to question number 9 regarding digital signatures, if you indicated that you do not make use of digital signatures; can you please elaborate why not?

Twenty four staff members did not know how to activate and use digital signatures in the e-mails. Two staff members did not see a reason why they should add a digital signature to their e-mails because they did not consider the e-mails to be confidential.

43. What Virus Scanner is installed on your work PC?

Only seven staff members interviewed, knew the default virus scanner installed on all NMMU's systems is Trend Micro OfficeScan. One staff member acknowledged using McAfee and another acknowledged using Norton Antivirus.

44. Explain what you know about the following:

- Virus

All staff members interviewed knew that a virus is a program that can damage a system, its hardware and its software.

- Worm

Seventeen staff members said that a virus and a worm have the same characteristics and the same purpose. The rest of the staff members interviewed did not know what a worm is or what it does to an infected system.

- Trojan horse

The majority of the staff members did not know what a Trojan horse is or what it does. One staff member said it has the same characteristics and the same purpose as a virus and another staff member said it is a program that hides and becomes active when ready.

4 DISCUSSION

The following is a brief overview of significant issues highlighted by the survey:

- The NMMU E-mail Policy and the NMMU Information Security Policy are created to provide management direction and support for e-mail and information security in accordance with business requirements and relevant laws and regulations. The policy states what is allowed and what is not allowed within the organisation by any NMMU e-mail account holder. Having and maintaining this policy is not enough. A sound policy needs to be refined over time to adjust for regulatory requirements, business strategy changes and changes in risk. At the NMMU it is clear that most staff members are aware of this policy but **only a few have read this** (ISO SANS 17799, 2005).
- Most interviewees were unaware of **how important** the information is that they are working with.
- The majority of staff members cannot differentiate between "**normal**" information and **confidential** information. Staff members could thus be sending confidential work related information to unauthorized users without their knowledge.
- None of the staff members knows the risks and counter measures associated with using non-NMMU laptops, mobile devices or personal

computers to access business related information. This could pose a risk if staff members access their e-mail accounts from such devices. On the NMMU Information Security website there is a clear description of the consequences when using non-NMMU laptops, mobile devices or personal computers. The website also provides for a step- by-step procedure on how to secure these devices and the connections it uses to access the internet e.g. setting up a VPN (Virtual Private Network), enabling encryption, enabling digital signatures. Clearly the information security content on the website should be "marketed" more internally.

- Only a handful of staff members use disclaimers in the e-mail they send. A disclaimer is a statement denying responsibility intended to prevent civil liability arising for particular acts or omissions. By adding a disclaimer in an e-mail, it could limit the damage after information has been breached and could save NMMU legal fees and save valuable time (Buys, 2004).
- The staff members showed a great uncertainty and lack of knowledge on encryption and digital signatures. The need for encryption and digital signatures is overlooked by the fact that they do not consider the information they work with to be important. A step-by-step procedure is provided on the NMMU Information Security website to show how to activate these features.
- Only a handful of staff members are aware of the virus scanners installed on the system and the current state of it. Most of the staff members have to open e-mails from unknown people or sources. They receive requests for information on students or staff members that have to be processed and routed to the appropriate person. Staff members also use their work e-mail account for sending and receiving personal related e-mails. The use of a virus scanner on these staff members' system is a must. They place the NMMU networks and systems in great danger by continuing to use their e-mail accounts and virus scanners in this manner.
- The sharing of personal passwords is one of the greatest threats to the three components (confidentiality, authentication and integrity) of information security. The staff members clearly indicated that password selection is not seen as an important factor. The key factors when selecting passwords are overlooked. No attention is given to

maximum lengths, permitted characters, etc. and this makes it easier for an unauthorized person to get access to a staff member's password. During the interviews some staff members thought it was acceptable to give the researcher his/her password for examination. Passwords should **never be shared with anyone for any reason.**

5 CONCLUSION

Staff members must become more aware of the following:

- NMMU Information Security website and its contents
- NMMU E-mail Policy and NMMU Information Security Policy
- Confidentiality, integrity and availability of information
- Control mechanisms (features) to protect information
- Encryption and digital signatures
- Virus Scanner and threats associated with it
- Password selection and proper use thereof

Being security aware means a person understands that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the data that is e-mailed within an organisation's computer systems and throughout its organisation. From the findings it is clear that there is very limited e-mail security awareness at NMMU in the Registrar's Division. The staff members who were interviewed had hardly any interest in securing the information that they work with and were completely unaware of the consequences of unprotected information. The guidelines and tutorials available on the NMMU Information Security website are not used properly or not used at all. This places NMMU in a very difficult situation with regards to securing valuable information and could lead to the downfall of this organisation.

Encryption and digital signatures are easy ways of ensuring that information sent and received by staff members remains confidential whilst integrity is ensured. The staff interviewed made it clear that they have no interest in making use of these features. The implementation of these two features reduced the risk of unauthorized viewing and altering by a great percentage. Located on the NMMU Information and Security website is a step-by-step procedure on the implementation and use of

encryption and digital signatures within the domain (Cisco Networking Academy, 2005).

A Virus Scanner is considered the first line of defence against all known threats (virus, worm and trojan horse). An in depth knowledge of the Virus Scanner is not needed, but the knowledge of the existence and its current state is. From the findings it is clearly stated by most staff that there is a great lack of knowledge of the current Virus Scanner and the current state of it (Whitman and Mattord, 2007).

The staff interviewed stated that they had not received any form of information security training. Staff members need to attend security workshops, presentations or awareness courses. After the attendance of a security workshop, presentation or awareness course, they need to be reminded of the security aspect on a regular basis. This will ensure continues awareness of information security related matters and the consequence of improper management of information.

6 REFERENCES

Buys, R (2004) *E-mail disclaimers explained.* Available from: http://www.buys.co.za/ (Accessed 15 June 2008).

Cisco Networking Academy. (2005) *CCNP2: Remote Access - 3.1*. Available from: https://cisco.netacad.net/ (Accessed 21 February 2008).

Kvale, S (1996) *InterViews - An Introduction to Qualitative Research Interviewing*. SAGE Publications, Inc.

Olivier, M.S. (2004) *Information Technology Research - A Practical guide for Computer Science and Informatics* 2nd edition. Van Schaik Publishers, Pretoria.

South African National Standard. (2005) *SANS 17799:2005 Edition 2. Information technology – Security techniques – Code of practice for information security management.* Standards South Africa.

Whitman, M.E and Mattord, H.J. (2007) *Principles of Incident Response and Disaster Recovery.* Thomson Course Technology.