

بسم الله الرحمن الرحيم

Sudan University of Science and Technology

College of Graduate Studies

***A proposed Security Framework for Portable
Media Devices. A Case Study of Sudanese Banks***

إطار عمل مقترح لتأمين الأجهزة المحمولة النقالة.

دراسة حالة في المصارف السودانية

**A thesis submitted in partial fulfillment of the
Requirements for the degree of M.Sc in Computer Science**

Prepared by:

Mussab Elagib Abass Hamza

Supervisor:

Dr. Mohamed Awad

2010

آية

بسم الله الرحمن الرحيم

قال تعالى

(وَيَسْئَلُونَكَ عَنِ الرُّوحِ قُلِ الرُّوحُ مِنْ أَمْرِ رَبِّي وَمَا أُوتِيتُمْ مِنَ
الْعِلْمِ إِلَّا قَلِيلًا).

صدق الله العظيم .

سورة الأسراء ، آية (85) .

DEDICATION

To my..

Father

Mother

Brothers

Sisters

And all friends

ACKNOWLEDGEMENT

I would like to thank My supervisor Dr. Mohamed Awad for his experience, skillful guidance.

Specially thanks are extended to proff.Ez Eladeen .

I owe thanks to Dr. Wesal El Tingary.

My especially thanks go to IT staff of brakka banks.

Finally my thanks and apologies to all of the kind people who have helped me but whose names have not mentioned.

Abstract

Portable media device spread few years ago. They are cheap and light weight what make them accessible for the staff. They also participate in increasing companies productivity moreover they are suitable for all situation and time, though they have many disadvantages if the users do not follow the right principles when dealing with them in a correct way that might lead to counter-productive.

The thesis aimed to study the types of removable device and the problems that the users might face at the abuse of these devices and the internal threats caused by the users also the study to the previous studies in this realm as well as information security in general.

The thesis objectives contain a questionnaire which check whether there are systems to control the work using removable devices also to find if there are problems while use these devices, and design security framework and how to control and apply them in banks.

At the end of this thesis there is a summary and recommendations for further work in this field.

المستخلص

بدأت الأجهزة القابلة للإزالة تنتشر في السنوات القليلة الماضية ، وهي رخيصة الثمن وخفيفة الوزن ، وهذا من الأسباب التي جعلتها أن تكون في متناول جميع الموظفين،وقد ساعدت في زيادة الإنتاجية بالنسبة للمؤسسات، وكذلك ساعدت الموظفين في العمل في أي مكان وأي زمان.

لكن هذه الأجهزة يمكن أن تتسبب في مضار كثيرة إن لم نتحكم في التعامل معها بصورة جيدة بواسطة أسس وسياسات معينة، كذلك إن لم نستخدم سياسات وضوابط يمكن أن تكون هنالك نتائج عكسية عند إستخدام هذه الأجهزة.

هذه الأطروحة تحدثت عن أنواع الأجهزة القابلة للإزالة ،والمضار التي تواجهنا عند سوء الإستخدام،والمهددات الداخلية للبنوك بواسطة الموظفين. وكذلك المشاكل المتوقعة إن لم نتبع أسس وسياسات تضبط التعامل مع هذه الأجهزة. وكذلك تعرضت هذه الأطروحة للدراسات السابقة في هذا المجال.وتحدثت عن أمن المعلومات بصورة عامة .

أهداف هذه الإطروحة إطار عمل أمني للتعامل مع هذه الأجهزة ، وتطبيقه في البنوك.وإنشاء سياسات لضبط الأجهزة القابلة للإزالة وكذلك الحواسيب المحمولة.

وقد تم عمل إستبيان في البنوك السودانية لمعرفة هل هنالك سياسات لضبط العمل بواسطة الأجهزة القابلة للإزالة، وهل هنالك مشاكل تحدث عند إستخدام هذه الأجهزة ، وبعد مناقشة النتائج ، تم عمل إطار عام وسياسات لضبط العمل بواسطة هذه الأجهزة.

وفي نهاية هذه الأطروحة كان هنالك ملخص ، والتوصيات للعمل المستقبلي في هذا المجال.

LIST OF FIGURE

| | | |
|-----------------|---|----|
| Figure 1 | <i>Information security factor.....</i> | 7 |
| Figure 2 | <i>Framework procedure.....</i> | 42 |

LIST OF TABLES

| | | |
|---------------------|---|-----------|
| Table 2.1.1 | Organizational Assets..... | 5 |
| Table 2.4.1 | Information System lists vulnerabilities | 8 |
| Table 2.4.2 | Categorize threats to information assets..... | 9 |
| Table 4.4.1 | Using portable media devices | 21 |
| Table 4.4.2 | Portable media devices banks policies | 22 |
| Table 4.4.3 | Problem when using this devices | 22 |
| Table 4.4.4 | Damage procedures | 23 |
| Table 4.4.5 | License banks to use this devices | 23 |
| Table 4.4.6 | Policies sufficient and fair | 24 |
| Table 4.4.7 | Policies to mange devices | 24 |
| Table 4.4.8 | Portable media devices banks marked | 25 |
| Table 4.4.9 | USB flash mechanism | 25 |
| Table 4.4.10 | Antivirus scanning | 26 |
| Table 4.4.11 | Limit the access | 26 |
| Table 4.4.12 | Laptops passwords policies | 27 |
| Table 4.4.13 | Cipher techniques | 27 |
| Table 4.4.14 | Update antivirus software | 28 |
| Table 4.4.15 | Backup operations | 28 |

| | | |
|---------------------|---|-----------|
| Table 4.4.16 | Training courses | 29 |
| Table 4.4.17 | Satisfied training courses | 29 |
| Table 4.4.18 | Using laptops in public places | 30 |
| Table 4.4.19 | Laptops security software | 30 |
| Table 4.4.20 | Abolished unused ports | 31 |
| Table 4.4.21 | Password to access devices | 31 |

TABLE OF CONTENTS

| | |
|--|-----|
| CHAPTER 1: INTRODUCTION | |
| Dedication | III |
| Acknowledgement | IV |
| Abstract | V |
| 1.1 OVERVIEW | 2 |
| 1.2 Thesis Problem | 2 |
| 1.3 Thesis Objectives | 2 |
| 1.4 Importance of Thesis..... | 2 |
| 1.5 Thesis Methodologies | 3 |
| 1.6 Thesis Boundaries | 3 |
| CHAPTER 2: INFORMATION SECURITY | |
| 2.1 Introduction..... | 5 |
| 2.2 Information Assets | 5 |
| 2.3 The Concept. | 6 |
| 2.4 Vulnerabilities & Threats..... | 7 |
| 2.5 Information at Risk: | 10 |
| 2.6 data security Keys | 10 |
| 2.7 Document Security..... | 12 |
| 2.8 Encryption | 12 |
| CHAPTER 3: Mobile Devices Threats | |
| 3.1 Definitions of portable media devices (PSD)..... | 15 |
| 3.2 The rise of portable storage devices: | 16 |
| 3.3 Portable media devices..... | 16 |
| 3.4 Corporations protection..... | 17 |
| 3.5 Insider threat..... | 17 |
| 3.6 Data theft: | 17 |
| 3.7 Legal liabilities..... | 18 |
| 3.8 Productivity loss..... | 18 |
| 3.9 Corporate network security breaches..... | 19 |
| 3.10 Commonly used countermeasures..... | 19 |

| | |
|---|----|
| CHAPTER 4: Questionnaire | |
| 4.1 Introduction: | 21 |
| 4.2 Sample Size | 21 |
| 4.3 Results..... | 21 |
| 4.4 Discussions of the Results: | 21 |
| CHAPTER 5: Framework | |
| 5.1 Introduction | 33 |
| 5.2 General – all mobile devices: | 33 |
| 5.3 Physical security – all mobile devices: | 33 |
| 5.4 PDAs, USB Key/Flash drive memory sticks..... | 34 |
| 5.5 Laptops | 38 |
| 5.5.1 Introduction..... | 38 |
| 5.5.2 Rules and responsibilities: | 38 |
| 5.6 Passwords policy: | 39 |
| 5.7 Practical Tips to Prevent Theft: | 40 |
| 5.8 Benefits: | 41 |
| CHAPTER 6: CONCLUSIONS AND FUTURE WORK | |
| 6.1 Conclusions | 44 |
| 6.2 Future Work | 45 |
| REFERENCES | 46 |
| APPENDEX A | 47 |
| APPENDEX B | 53 |