**Security Risk Assessment For**

**ABC WIDGETS**

**Version 1.0**

**October 2020**

**Prepared for**

**ABC WIDGETS**

**Prepared By**

**Communications & Business Team**

**Table of Contents**

Table of Contents Page 2  
  
Executive Summary Page 3

Introduction

1.1 Purpose Page 4

1.2 Scope Page 4

Risk Assessment Approach

2.1 Participants Page 5

2.2 Techniques used Page 5-6

2.3 Risk Model Page 6

System Components

3.1 Technology components Page 7

3.2 Equipment in operation Page 7

Vulnerability Statement

4.1 Overview Page 8

4.2 Physical Vulnerability Assessment Page 8

4.3 Vulnerabilities identified Page 9

Threat Statement

5.1 Overview Page 10

5.2 Credible Threats Page 10-11

Results Page 11-13

Conclusion Page 14

Recommendations Page 14

References/Appendix Page 15

**Executive Summary**

The purpose of this report is to identify cyber security vulnerabilities and exploitations within the organization.

C&B Team have found multiple vulnerabilities within the organization itself these include:

* All servers and devices are running different and outdated operating systems
* Devices are running outdated patches creating vulnerabilities
* Sensitive data is stored on a single server
* Insecure protocols

**Action to be taken:**

* Mandatory training for staff and quarterly refresher training
* Ongoing weekly patch updates of all devices
* Consistency between operating systems on devices

**1.   Introduction**

**1.1**  **Purpose**

The purpose of this initial risk assessment is to evaluate and document the adequacy of the ABC Widgets security. This assessment provides a structured risk profile of the company, addresses current shortcomings and recommends improvements to mitigate the existing threats and vulnerabilities.

**1.2. Scope of this risk assessment**

The scope of this risk assessment included the physical location of the ABC Widgets, the IT systems and documentation to identify the threats and vulnerabilities and discover potential risks.

**2.  Risk Assessment Approach**

This risk assessment methodology was conducted using the guidelines in NIST SP 800-30, *Guide for Conducting Risk Assessments*. The assessment evaluates security vulnerabilities and threats and recommends appropriate security mitigation techniques.

**2.1 Participants**

Participants and their roles in this risk assessment were as follows:

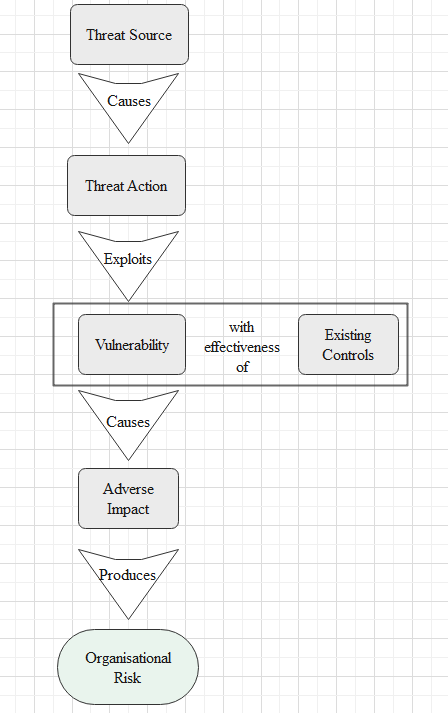
* **Pete Peterson,** ABC Widgets Data Owner, provided documentation and information through interviews.
* **Simone Simmonds,** ABC WidgetsSystems Owner, helped with staff interviews and questionnaires.
* **Julie Jones,** ABC Widgets Data Custodian, Network Manager and Database Administrator, provided necessary technical documentation and information about ABC Widgets.
* **Dominic Adams,** Member of the Risk Assessment Team, conducted interviews and documentation reviews.
* **Ronan O’Connor,** Member of the Risk Assessment Team, performed cyber hygiene checklist and physical vulnerability assessment.
* **Gary Godwin,** Member of the Risk Assessment Team, conducted interviews and Identified the IT System.
* **Deimante Krinickaite,** Member of the Risk Assessment Team, identified threats and vulnerabilities.

**2.2 Techniques Used**

|  |  |
| --- | --- |
| **Technique** | **Description of the Technique** |
| **Cyber Hygiene Checklist** | Performing checklist to gain a broad picture of the existing cyber security infrastructure at the ABC Widgets. |
| **Documentation reviews** | Reviewing the existing documentation and evaluating the compliance with policies and procedures. |
| **Interviews** | Conducting interviews with personnel to gain a further insight into compliance with policies and procedures and identifying the threats. |
| **IT System Identification** | Identifying the IT system components using existing documentation and additional information. This technique aids in defining the boundary of the risk assessment. |
| **Threat Identification** | Using NIST SP 800-30, interviews and documentation to define potential threats. |
| **Vulnerability Identification** | Evaluating the premises and physical components of the ABC Widgets, extracting the information from interviews and document reviews to identify the vulnerabilities. |

**2.3 Risk Model**

Risk models (as described in NIST SP 800-30) define risk factors that are assessed and relationship between them. Typical risk factors include threat, vulnerability, impact, likelihood and predisposing condition. In our case we used threats that were further divided into threat-source and threat-action, vulnerability, existing controls, impact and likelihood.

****

**3. System Components**

**3.1 Technology components**

|  |  |
| --- | --- |
| **Component** | **Description of the Component** |
| **Applications** | A file containing many scripts to present the user with an interface that does a specific thing. |
| **Databases** | A library of all information necessary for transactions, searches, and file requests. |
| **Operating Systems** | Software that allows a user to run applications and files on their device. |
| **Networks** | A communication web that allows devices to connect with each other. |
| **Security Alarm** | A device that produces a very loud continuous noise and contacts a contracted Security Agency when a trespasser is detected. |
| **Protocols** | Different procedures to transfer files and data over a network. |

**3.2 Equipment in operation**

The equipment used at ABC Widgets:

* EFTPOS (electronic payment system) terminals connected to file servers locally through WiFi using WPA.
* 3 MS Servers 2008 and 2 running MS Server 2012 (One

physical with 5 VM’s, 3 switches and two routers stored in the

administrator room).

* 30 client Computers. The computers are running different

operating systems, including Windows XP, Windows 7 and Windows 10.

* 5 printers and routers with access points, some of them have been

updated and patched to the latest version.

**4. Vulnerability Statement**

**4.1 Overview**

This Security Risk Assessment is the first of its kind for ABC Widgets. Vulnerabilities were identified conducting interviews, reviewing the documentation, performing physical assessment of the premises.The vulnerabilities identified should be reviewed during the next risk assessment to evaluate their validity. Vulnerabilities that combine with identified threats create a risk. Those risks will be listed in Risk Assessment Results.

**4.2 Physical Vulnerability Assessment for ABC Widgets**

|  |  |
| --- | --- |
| **Component** | **Description of the Component** |
| **Security Guard** | Guard is not versed in crimes act 1958, as he is searching customers as they enter/leave the premises. |
| **Access Control** | Several un-necessary Server-room Security FOBs are available. |
| **Locks** | Premises is locked after-hours. |
| **Sensitive Device Locations** | Some network devices are stored in potentially risky areas. |
| **Burglary Alarm** | There is no Burglary Alarm installed. |

**4.3 Vulnerabilities Identified for ABC Widgets**

|  |  |
| --- | --- |
| **Vulnerability** | **Description** |
| **Firmware** | Most of the Servers, Routers, and other end-points are not running up to date Firmware. Represents serious network security concerns. |
| **Password Policy** | No ‘Strong Password’ policy has been implemented, the network is incredibly vulnerable to ‘password attacks’. Employees are also not keeping passwords to themselves. |
| **WiFi Radius** | The WiFi has been poorly configured, as it is accessible from areas outside the store. |
| **Database** | Financial Data has been found to be stored in the same database as everything else to do with the store, allows attackers easy access to all customer and transaction records [SERIOUS LIABILITY ISSUE] |
| **File Transfer Protocols** | Wireshark has detected that transactions and other file transfers are not using SFTP, all secure transactions are being sent as plain-text. |
| **Electronic Billing** | EFTPOS machine is not running up to date firmware, and represents serious financial security vulnerability as it could easily be hacked.  [SERIOUS LIABILITY ISSUE] |

**5. Threat Statement**

**5.1 Overview**

The credible threats to ABC Widgets system were identified by analyzing documentation and interviewing appropriate staff members (Network Manager, ABC Widgets data owner) and using NIST SP 800-30 as a guideline to collect the information about threat sources and threat actions.

* **Threat source** - The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability. Common threat sources can be human, natural or environmental.
* **Threat action** - A method by which an attack may be performed.

**5.2 Credible Threats Identified for ABC Widgets**

|  |  |
| --- | --- |
| **Threat-Source** | **Threat Actions** |
| **Human** | Vulnerabilities in operating system on Servers and PCs open to known exploitation |
| **Human** | Exploitation of known vulnerabilities leaving transport protocols open to monitoring exposing client data |
| **Human** | Unpatched IoT devices creating weak spots in local network |
| **Human** | Database not segregated creating vulnerabilities to client data |
| **Human** | Shared passwords creating breach in access controls |
| **Human** | Easy to guess passwords open to brute force attempts |
| **Human** | FTP in use exposing information to spoofing, sniffing, brute force. |
| **Human, Environmental** | No access controls for server room |
| **Human, Environmental** | WiFi access reaching carpark opening networking to brute force attempts and sniffing. |
| **Human** | Wireless network outdated security protocols with known vulnerability exploits |
| **Human** | Lack of regular updates leaves the organization open to ransomware attacks. |

**6.  Risk Assessment Results**

Risk Assessment Results were presented in the table and the table contents include:

* Observation number and brief description of the observation
* A discussion of the threat-source and vulnerability pair
* Identification of existing mitigating security controls
* Evaluation of the likelihood
* Evaluation of the impact
* Risk rating based on the risk-level matrix
* Recommended controls or alternative options for reducing the risk.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Item Number** | | **Observation** | **Threat-Source/**  **Vulnerability** | **Existing controls** | **Likelihood** | **Impact** | **Risk Rating** | **Recommended controls** | |
| **1** | **Server OS outdated** | **Exploitation** | **N/A** | **High** | **High** | **High** | **Install latest OS** |
| **2** | **Electronic billing protocol outdated** | **Exploitation** | **N/A** | **Medium** | **High** | **High** | **Update to WPA2 (Enterprise)** |
| **3** | **PC OS outdated** | **Exploitation** | **N/A** | **High** | **High** | **High** | **Update OS** |
| **4** | **Printer outdated patch** | **Exploitation** | **N/A** | **Low** | **Medium** | **Medium** | **Run automatic updates or set weekly schedule** |
| **5** | **Routers outdated patch** | **Exploitation** | **N/A** | **High** | **High** | **High** | **Run automatic updates or set weekly schedule** |
| **6** | **Non-segregated data storage** | **Vulnerability** | **N/A** | **Medium** | **High** | **High** | **Separate financial data from other business data with secondary server** |
| **7** | **Shared passwords** | **Social Engineering** | **N/A** | **Medium** | **High** | **High** | **Reset all passwords, Educate staff.** |
| **8** | **Weak passwords** | **Vulnerability** | **N/A** | **High** | **High** | **High** | **Implement minimum criteria for passwords reset password after X time has passed.** |
| **9** | **FTP plain-text** | **Vulnerability** | **N/A** | **High** | **High** | **High** | **SSH only file transfer** |
| **11** | **Server room lacks access control measures** | **Social Engineering** | **Swipe cards** | **Low** | **High** | **Medium** | **Track all swipe cards and/or restrict number of swipe cards** |
| **12** | **WiFi extends to carpark** | **Vulnerability** | **N/A** | **Medium** | **High** | **Low** | **Change WiFi access radius, possible remove unnecessary WAPs** |
| **13** | **Wireless network outdated security protocols** | **Exploitation** | **WPA** | **High** | **High** | **High** | **Update to WPA2 (Enterprise)** |
| **14** | **Lack of data backup** | **Vulnerability** | **Behind locked closet** | **High** | **Medium** | **Medium** | **Weekly data backups** |
| **16** | **Alarm system** | **Environment** | **N/A** | **High** | **Medium** | **High** | **Install an alarm system** |

**7. Conclusion**

ABC Widgets is suffering from an extensive series of both hardware and software vulnerabilities. Immediate implementation of suggested controls is necessary to minimise threat vectors and potential for data loss or theft.

**8. Recommendations**

***8.1 Cyber Security Policy***

* Update to WPA2 Enterprise
* Install newest and regularly update OS
* Set and perform automatic updates
* Segregate financial data on separate data server
* Update and employ password policy

***8.2 Cyber Security Awareness Strategy***

* Mandatory security meeting for each department
* Email employees updated password policy

***8.3 Cyber Security Training***

* Security training on hire with refresher every three months

***8.4 Best Practice Hygiene***

* Install and update antivirus and antimalware
* Use adequate firewall protections
* Perform regular software updates
* Employ strong password policy
* Encrypt data transfers
* Perform regular back-ups

**9. References/Appendix**

***9.1 Peer review of Team***

Gary Godwin:

1. Is the report clearly written? Yes
2. Are all sections filled validly? Yes
3. Is the structure and layout logical? Yes
4. Is all data accurate? Yes
5. Additional comments? No

Ronan O’Connor:

1. Is the report clearly written? Yes.
2. Are all sections filled validly? Yes.
3. Is the structure and layout logical? Yes.
4. Is all data accurate? Yes.
5. Additional comments? No.

Deimante Krinickaite

1. Is the report clearly written? Yes
2. Are all sections filled validly? Yes
3. Is the structure and layout logical? Yes
4. Is all data accurate? To our knowledge - Yes
5. Additional comments? n/a

Dominic Adams

1. Is the report clearly written? yes
2. Are all sections filled validly? yes
3. Is the structure and layout logical? yes
4. Is all data accurate? to a reasonable level
5. Additional comments?

***9.2 References***

[www.owasp.org](http://www.owasp.org)

[www.cyber.gov.au](http://www.cyber.gov.au)

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf