**PROJECT 5**

**Title: DHAEI Risk Management Case Study**

***By Titobiloluwa (Tito) Ilori***

**Executive summary**

DHAEI, as a company that provides internet access, website registration and hosting alternative, wants to ensure that all its systems meet a minimum level of security and that its information is protected from attacks. The company will also need a way to collect and act on security events from across its digital estate or branches. The research was carried out on the infrastructure to identify the risk associated with the assets to determine what more is needed to be done for an improved security posture.

Relevant information to decide vulnerability and threats that are applicable was gathered by meeting with asset owners. Other vulnerabilities were identified using a Cyber Threat Intelligence site (MITRE CVE and NIST NVD). We provided measures to be taken to mitigate the threat identified using the ISO 27001:2013 Annex A Control14. Mostly, the control measures will include providing secure encryption for the VPN-enabled laptops, installing patches (security updates) on the WSUS server and providing training to clients, for the use of the desktop Windows computers they have access to in all the offices.

CLASSIFIED: **CONFIDENTIAL**

**Risk Assessment and Risk Treatment Methodology**

**1. Purpose, Scope, and Users**

This document aims to define the methodology for assessing and treating information risks in DHAEI - a software development company based in the Durham area and to define the acceptable level of risk according to the ISO/IEC 27001 standard.

The risk assessment and risk control/treatment are applied to the entire scope of the Information Security Management System (ISMS) of the company with provides internet access, web registration and hosting alternatives to its clients.

The users of this Risk Management Plan document are all employees of DHAEI who take part in Risk Assessment and risk management.

**2. Risk Assessment and Risk Treatment Methodology**

**2.1 Risk Assessment**

**2.1.1. The Process**

I interacted with the document supplied for the project. Meanwhile, I would involve Paul Alexander (CISO) for more information about the security measure already implemented in the IT infrastructure. I would also involve the COO (Richard Xavier) and a group of other users/employees in operations and development to understand to kind of data and configuration/version/build IT devices they use.

**2.1.2. Assets, Vulnerabilities, and Threats**

Steps were taken here to identify the assets and research the known vulnerabilities and consider the common vulnerability associated with them. Three of the assets were selected for the project. These are listed in the table below.

| # | **Asset** | **Threat** | **Vulnerability** |
| --- | --- | --- | --- |
| 1 | **Company-issued Laptops** | DOS Attacks2 | Unencrypted L2TP (CVE-2023-21757; CVE-2023-21679) 1,2,3 |
| MiTM Attacks |
| Data Interception |
| Remote Code Execution3 |
| 2 | **WSUSI = Windows Software Update Services (WSUS) server 2019** | Data Breach | Windows Elevation of Privilege Vulnerability; CVE-2023-32056; CVE-2023-35317 4,5,6 |
| System Compromise and Control |
| Process Injection |
| 3 | **Data on Desktop Workstations** | Phishing | Accessing email on the desktop |
| Data loss/theft | Removable media, unattended device |

**2.1.3. Determining the Risk Owners**

In the table below, I will highlight the asset owners and risk owners for the assets listed above.

| **Asset** | **Asset Owner** | **Risk Owner** |
| --- | --- | --- |
| ***Company-issued Laptops*** | Scotty Doohan - Mgr. Applications | Paul Alexander - CISO |
| ***WSUSI Winserver 2019*** | William Freund - Mgr. Systems | Paul Alexander - CISO |
| ***Data on Desktop Workstations*** | Paul Alexander - CISO | Paul Alexander - CISO |

In the first assets, the description says about 20 programmers work from home offices using company-issued laptops. The developers/programmers are in the Applications department reporting to the Manager of Applications.

WSUSI is one of the systems in use within the organisation which system software updates which I believe will be owned by the Manager of Systems.

The data/information of the clients and the company will be preserved and its risks will be mitigated by the Chief Information Security Officer.

**2.1.4. Impact and Likelihood**

| # | **Asset** | **Threat** | **Impact** | **Likelihood** | **Risk Lvl** |
| --- | --- | --- | --- | --- | --- |
| 1 | **Company-issued Laptops** | DOS Attacks2 | **8** | **4** | **12** |
| MiTM Attacks | **7** | **3** | **10** |
| Data Interception | **7** | **3** | **10** |
| Remote Code Execution3 | **8** | **3** | **11** |
| 2 | **WSUSI = Windows Software Update Services (WSUS) server 2019** | Data Breach | **7** | **4** | **11** |
| System Compromise and Control | **7** | **3** | **10** |
| Process Injection | **7** | **2** | **9** |
| 3 | **Data on over 2, 000 Desktop Workstations** | Phishing | **6** | **3** | **9** |
| Data loss/theft | **6** | **2** | **8** |

**2.2. Risk Acceptance Criteria**

1. The risk associated with company-issued laptops is high given the CVSS base scores of 8.17 and 7.58 and it is important to provide a system-specific control for the devices. This also poses a high threat to the CIA triad. Controls are listed in section 2.3.1 below.
2. The risk assessment of the Windows Software Update Services (WSUS) server (using Windows Server 2019) also shows high impact and exploitability levels in the NIST National Vulnerability Database5,6. A control should also be provided for this item in addition to the aforementioned risk.
3. The last set of assets shows a medium risk level. I will also potentially recommend that **A.5.1.1** control should also be implemented for it as shown in the Risk Treatment section below.

**2.3. Risk Treatment**

Primarily, I will be using the ISO 27001:2013 Controls.

I will prioritize the risk treatment of L2TP VPN connections of the Company-issued laptops for the programmers as it poses more impact on the company’s infrastructure, systems, and data protection.

I would also recommend that the company update their desktop Operation System that is currently running Windows 10 which is outdated.

Here is the order of priorities and the respective controls or treatments.

**2.3.1: L2TP VPN connections of the Company-issued laptops:**

| **Annex A reference** | **Control title** | **Control description** |
| --- | --- | --- |
| **A12.5.19** | Installation of software on operational systems | Procedures shall be implemented to control the installation of software on operational systems. |
| **A14.1.210** | Securing application services on public networks | The information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. ***USING IPSec or TLS/SSL encryption.1*** |

**2.3.2: Windows Software Update Services (WSUS) server (Windows Server 2019)**

| **Annex A reference** | **Control title** | **Control description** |
| --- | --- | --- |
| **A12.2.19** | Controls against malware | Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. |
| **A12.6.19** | Management of technical vulnerabilities | Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. |

**2.3.3: Data on over 2,000 Desktop Workstations in Main Office and Branch offices**

| **Annex A reference** | **Control title** | **Control description** |
| --- | --- | --- |
| **A.5.1.111** | Policies for information security | A set of policies for information security shall be defined, approved by management, published, and communicated to employees and relevant external parties. |
| **A.8.3.112** | Management of removable media | Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. |
| **A11.2.813** | Unattended user equipment | Users shall ensure that unattended equipment has appropriate protection. |

**3. References**

1. Understanding Layer 2 Tunneling Protocol (L2TP) - by Rachel Lee (March 14, 2023) <https://vpn.surf/blog/l2tp-protocol/>
2. CVE-2023-21757 Detail - NIST NVD (April 27, 2023) - <https://nvd.nist.gov/vuln/detail/CVE-2023-21757>
3. CVE-2023-21679 Detail - NIST NVD (April 27, 2023) - <https://nvd.nist.gov/vuln/detail/CVE-2023-21679>
4. Process Injection - MITRE ATT&CK (March 30, 2023) - <https://attack.mitre.org/techniques/T1055/>
5. CVE-2023-32056 Detail - NIST NVD (July 14, 2023) - <https://nvd.nist.gov/vuln/detail/CVE-2023-32056>
6. CVE-2023-35317 Detail - NIST NVD (July 14, 2023) - <https://nvd.nist.gov/vuln/detail/CVE-2023-35317>
7. Common Vulnerability Scoring System Calculator CVE-2023-21679 - NIST NVD - <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2023-21679&vector=AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H&version=3.1&source=Microsoft%20Corporation>
8. Common Vulnerability Scoring System Calculator CVE-2023-21757 - NIST NVD - <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2023-21757&vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H&version=3.1&source=Microsoft%20Corporation>
9. ISO 27001 Annex A.12.1 Operational Procedures and Responsibilities - <https://www.isms.online/iso-27001/annex-a-12-operations-security/>
10. ISO 27001 – Annex A.14: System Acquisition, Development & Maintenance - <https://www.isms.online/iso-27001/annex-a-14-system-acquisition-development-and-maintenance/>
11. ISO 27001 – Annex A.5: Information Security Policies - <https://www.isms.online/iso-27001/annex-a-5-information-security-policies/>
12. ISO 27001 – Annex A.8: Asset Management - <https://www.isms.online/iso-27001/annex-a-8-asset-management/>
13. ISO 27001 – Annex A.11: Physical & Environmental Security - <https://www.isms.online/iso-27001/annex-a-11-physical-and-environmental-security/>
14. ISO 27001 – Annex A Controls - <https://www.isms.online/iso-27001/annex-a-controls/>