**Aim of the project**

This project will undertake a minimally-invasive cyber-security risk assessment of a company’s IT Infrastructure.

This will allow any vulnerabilities to be identified and mitigated.

The target company, European Automotive Technology (EAT) is a small(ish) company operating in Hobart. It services Automotive Vehicles, particularly the European marques as well as undertaking bodyworks. They have an excellent reputation locally.

The company’s existing IT infrastructure comprises 1 server, 2 PCs (with laptops occasionally connected to the network.) along with associated routers, switches, Modems, Printers etc.

They also have a web presence (website).

**Objectives of the project**

This project will undertake a thorough investigation of the existing IT Infrastructure of EAT.

This will include any IT Infrastructure item comprising the entire Local Area Network of EAT

The investigation will be minimally intrusive in that it will be an information gathering only investigation with NO penetration testing.

From the information gathered above, any vulnerabilities identified will be fully investigated and a comprehensive mitigation strategy developed to eliminate or significantly reduce those vulnerabilities.

**Justification**

The existing IT infrastructure at EAT has been in place for a significant number of years and has been updated as required on an ad-hoc basic. The company IT Infrastructure is supported externally and appears to be operating in a satisfactory manner but the increasingly hostile cyber environment suggests that the risk of a successful cyber attack is becoming more and more likely as time goes on.

The software and hardware required to undertake normal business operations has become more complex over time and the freely available tools needed to undertake a successful hack are becoming more and more powerful. This means that continuing to operate the Network in the same manner as in the past may leave EAT exposed to a successful cyber-attack.

Given the increasingly hostile cyber environment the risk assessment will identify any significant vulnerabilities in the current configuration and allow mitigation strategies to be implemented to provide greatly enhanced security against a successful cyber-attack for the short and medium term future.

**Scope**

## **In Scope**

All relevant equipment comprising the clients, including Servers, PCs, laptops, tablets, routers, switches, modems, wi-fi router devices, printers, ethernet ports.

This includes

## ***Hardware***

* Physical Security
* Hardware
  + Make
  + Model
  + Version No
  + Firmware (if applicable)

## ***Software***

* + Name
  + Version No
  + Update Status

## ***Configuration Files e.g.***

* + Firewall settings
  + Antivirus settings

## ***Security Settings e.g***

* + Wi-Fi encryption standard
  + Password standards (simple, complex, retention period)

## ***File/Folder Security***

* + Access Lists
  + Share Security

## **Out of Scope**

## ***Phones***

while employee phones may connect to the network and hence present a risk, this may be considered too intrusive to pursue.

## ***Software Suitability***

No investigation will be undertaken as to whether existing software is well suited to the task or whether a better suite of software is available.

## ***Penetration Testing***

No penetration testing of the network will be undertaken as this is considered to be too intrusive and may, inadvertently, cause one or more existing services to fail.

Testing will not include altering any of the running software or software configurations on the machine. This project will only perform inspections on the systems to minimise the possibility of any interruption of service to the client.

**Proposed methodology**

## **Testing Methodology**

Where possible (PCs, Laptops) the assessment will be made by sitting down at the device and recording information which is relevant to the (cyber) security of that device.

For the server and other non-directly accessible machines (router etc), in order to minimise disruption to the normal operations of the firm I will use my laptop to remotely access these devices.

For other equipment (printers etc) I will print status information and or inspect visually to obtain make model and version no.

## **Management Methodology**

For this project I will be using a traditional waterfall methodology, monitoring progress and adjusting the Gant chart as required.

Given that this is a very short project, updates will be required at least weekly.

**Risks** (Kloppenborg, T et al, 2018 p366-377)

The existing risks have been identified and given an Existing Level of Risk as seen in the following table.

. This level of risk is based on the Risk Matrix (Kloppenborg, T et al, 2018, p371) which is attached as Appendix A.

**Resources**

I will be the sole human resource for this project and will be using the following additional resources: -

|  |  |  |
| --- | --- | --- |
| **Hardware** | **Name/Version** | **Use/Purpose** |
| Laptop | COLIN-LAPTOP | Connecting to the LAN and interrogating devices which cannot be accessed directly. |
| Desktop | DESKTOP-A89UGLD | Documentation of Project |

|  |  |  |
| --- | --- | --- |
| **Software** | **Name/Version** | **User/Purpose** |
| MS Project | 2000 | Create a Gant chart of the project and update as project timelines change |
| MS Office | 2019 | Document all assessment findings and write resulting report. |
| Sublime-Merge |  | Track versions of all documents created |
| Endnote | Web | Document references used and produce suitably formatted output of those references. |

**Project schedule**

**Legal, ethical or social considerations**(Baloch, 2014),(Weidman, 2014

Prior to commencing the risk assessment, a signed agreement must be in place.

This will include permission for the risk assessment to take place and for the resulting report to be submitted to Edith Cowan University for assessment.

A non-disclosure agreement whereby the information resulting from the risk assessment will be kept secure (in an encrypted folder) and dissemination limited to the assessor, the client and Edith Cowan University (for the purpose of assessment).

The primary aim of this risk assessment is to determine the vulnerabilities of the client’s target system and make recommendations which will ensure that the target system, once remediation has occurred, will be more secure and less likely to be penetrated.

It is important that the assessor keep to the terms of the agreement and not extend the investigation in any way.

All communications between the attacker and the client should be secure (e.g. encrypted emails or hand delivered) and all the information resulting from the risk assessment should likewise be secure.

After the final report has been presented to the client and the final assessment submitted to Edith Cowan University for assessment all information (logs, notes, reports etc) should be deleted.

**References**

References should be provided for the background literature (APA style).