Activity-2 Identify threats

|  |  |
| --- | --- |
| Name: | Nathan Bransby |
| Student ID: | V141198@tafe.wa.edu.au |

# Part 1: Disposing of old PCs

Can you suggest any possible security risks to an organisation associated with the disposal or recycling of old computer equipment?

|  |
| --- |
| If the hard drive was not wiped correctly (or destroyed), it may allow someone to recover data from the hard drive and access:   1. Financial & Personal Information 2. Company Sensitive Information 3. Private Company Networks / Remote Connections |

# Part 2: Essential 8

What is the Essential 8?

|  |  |  |
| --- | --- | --- |
| The Essential 8 are 8 steps developed by The Australian Signals Directorate for businesses to mitigate cyber security threats. They Are:   * patch applications * patch operating systems * multi-factor authentication * restrict administrative privileges * application control * restrict Microsoft Office macros * user application hardening * regular backups.  |  |  | | --- | --- | | Source: | https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained | |

# Part 3: BYOD

Can you think of any security risks associated with staff using their own devices on the company network?

|  |
| --- |
| * A malicious actor gaining remote access to the device whilst connected to company intranets. * No anti-virus software installed potentially infecting other devices within the organisation. * Obtaining access to private information & client/staff information. * Attacking company network systems & denying access to systems (DDos) |