Device and Risk Register



1. Complete the table with the level of risk, gaps identified and risks that you can see from the type of data stored on each device. Below the table you will make any recommendations based on your assessment of the risk and any gaps that you have identified.
2. The first entry has been done as an example.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Staff Name/ Device operator**
 | 1. **Device Name**
 | 1. **Mac Address**
 | 1. **Malware installed**
 | 1. **VPN in use**
 | 1. **Device encrypted**
 | 1. **Data stored on the device**
 | 1. **Level of risk**
 | 1. **Gaps Identified**
 | 1. **Risks to consider**
 | 1. **Security protocol to apply**
 | 1. **Date**
 |
| Con Kafatos | Laptop 1001 | 00-3B-3S-F5-C3-D2 | Yes | Yes | Yes | Passwords for serverPasswords for emailAccess to cloud storage (auto login)Device passwordCompany staff registry | Catastrophic | None | Storage of a lot of company-sensitive data – passwords and server access | Quarantine deviceChange all passwordsFull systems analysis and report on the level of infiltration | Today |
| Con Kafatos | Tablet 2001 | 95-34-D3-Q2-G8-5B | No Yes (15/02/23) | No | Yes | Passwords for serverEmail loginsCompany staff registry | Moderate | None | Server access | Quarantine deviceChange all passwordsFull systems analysis and report on level of infiltration |  |
| Sally Fischer | Laptop 1002 | 67-O4-P1-C7-4R-G1 | Yes | Yes | Yes | Email passwordsLogin for central IT systemRouter configuration loginAccess to cloud storage | Moderate | None | Router config and login | Quarantine deviceChange all passwordsFull systems analysis and report on level of infiltration |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Tan Yamamoto | Desktop 3001 | 9G-67-D3-34-89-M1 | Yes | No | Yes | Software development loginsEmail loginsCloud storage loginSoftware in development – prototypes | Catastrophic | VPN not in use | Software in development | Quarantine deviceChange all passwordsFull systems analysis and report on level of infiltration |  |
| Tina Yates | Desktop 3002 | 4F-56-V3-L9-D3-12 | Yes | No | Yes | All staff profilesAccounting software loginsBank account loginsHR management files | Catastrophic | VPN not in use | Staff detailsHR detailsBank account info | Quarantine deviceChange all passwordsSet up two-factor authenticationFull systems analysis and report on level of infiltration |  |
| Sam Tailor | Laptop 1003 | 56-M2-12-B4-A4-C9 | No | Yes | Yes | Email loginsCloud storage login | Minor | Malware is not up to date | Email loginsData storage login | Quarantine deviceChange all passwords Anti-malware to be installed on auto-update settings. |  |
| James Hanson | Desktop 3003 | 89-09-Q1-N4-DF-56 | Yes | No | Yes | Email loginsCloud storage loginGraphic design templates | Moderate | VPN not in use | Email loginsData storage login | Quarantine deviceChange all passwords |  |
| James Mollison | Desktop 3004 | 34-T5-Y6-23-Q1-98 | No | Yes | Yes | Email loginsCloud storage login | Minor | Malware now configured | Email loginsData storage login | Quarantine deviceChange all passwordsAnti-Malware to be installed on auto-update settings |  |

|  |
| --- |
| 1. **Recommendations based on the findings of the gap analysis**

Identify any gaps and remedies here. Note that all data is not available in this table, and you may recommend some processes that are not identified and recommend that they be included in future gap analysis.(Approximate word count: 100 – 150 words) |
| The student must be able to identify that there are significant risks associated with these devices. There is a lot of sensitive and confidential information stored on them. There are no major gaps, but there could be a suggestion to tighten processes, encryption, two-factor authentication or other methods to ensure that each and every device is secure. Some data is missing, and the student may identify gaps or unknowns and make recommendations based on that. Gaps may include things such as malware not being up to date, VPN not in use, and emails needing two-factor password authorisations. Con Kafatos’ device would need an automatic update to ensure his Malware is always up-to-date. |
| 1. **Three-monthly Review**

Based on the instructions received from Con, you will review the information you have about the new staff member, James Mollison and input his details into the table above. Review the security breach and make recommendations to contain and address the breach. You must also identify what Con should do about his concerns over unauthorised credit card transactions and make any recommendations here.(Approximate word count: 100 – 150 words) |
| 1. James Mollison’s security breach.

The student must be able to identify a solution for James Mollison’s device and make recommendations, such as devices being set up in a central location and not by staff individually. Ensure all staff have an automatic update selected for their malware software to ensure it does not expire, installation of a new anti-virus and spyware software, further controls to systems and further limitations to application privileges. 1. Con Kafatos’ unauthorised credit card transactions.

Since Con Kafatos’ devices have had an automatic update for the past three months, there will have been no further issues with his malware. Regarding Con’s unauthorised transactions, this is not caused by using a company device. It is triggered by the credit card company. Recommendations include setting up two-factor authentication within the account of the credit card company. |