**Goals**

SecureTech has identified **five security concerns** that could lead to data breaches, operational disruptions, or compliance failures.

1. Access Control Risk
2. Asset Management Risk
3. Incident Management Risk
4. Physical Security Risk
5. Data Protection Risk

**The Goals of this assessment are to:**

1. Identifying the threat sources of each security concern
2. Identifying resulting events that may occur from the identified threat sources
3. Providing resolutions through mitigation/prevention strategies for each threat source

**Risk Assessment**

**Table of Threats, Hazards and Mitigation**

*This risk assessment follows the NIST 800-30 Guidelines:*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk | Threat Source | Threat Event (Characterised by TTPs) | Likelihood | Impact | Risk | Mitigation/Prevention Strategy |
| Access Control Risk | **Adversarial**  Individual - Insider:  Sharing of login credentials for internal systems to “save time” | -Mishandling of critical and/or sensitive information by authorised user  -Spill sensitive information  -Obtain unauthorised access  -Compromise software of organisational critical information system | Very High | Very High | Very High | -Add a “Consequence Management system” for any sharing of passwords  -Develop organisational wide awareness lessons and training on the importance of credentials and the threats sharing follows.  -Add 2FA  -Monitoring of who, when and where a login occurs |
| Asset Management Risk | **Structural**  IT Equipment - Storage:  No formal inventory existing for IT Assets | -Cause deterioration/destruction of critical information system components and functions  -Lack of awareness of Assets  -Inadequate protection of records with regards to information security and sensitivity | Moderate | Moderate | Moderate | -Create inventory list of IT Assets  -Frequent stock checks |
| Incident Management Risk | **Structural**  IT Equipment - Communications:  No clear process for reporting security incidents | -Threat of attacks going unreported  -Allow prolonged spread of infectious malware with lack of clear report systems in place | High | Very High | High | -Create reporting system for organisation  -Develop organisational wide awareness and training on signs of threats and what to do in the case of a given sign.  -Have frequent IT staff checks and scans of organisation computers and networks for security incidents  -Improve Surveillance for physical security incident threats |
| Physical Security Risk | **Structural**  Environmental:  Office servers are stored in an unlocked room accessible to all employees | -Exploitation of physical access of vulnerable integral areas to gain access to organisational facilities  -Compromise of critical information systems via physical access | High | Very High | High | -Add locks to server doors  -Limit access to authorised personnel only  -Security staff to physical in-moment protection  -Surveillance in, on and around server rooms |
| Data Protection Risk | **Structural**  IT Equipment -Storage:  Customer data stored unencrypted in unbacked cloud storage | -Exploitation of vulnerabilities in information systems due to lack of encryption.  -Exploit insecure or incomplete data deletion in insecure cloud environment  -Easy threat of exfiltration of data/information due to lack of encryption  -Threat of loss of data/information due to unbacked data storage | Very High | Very High | Very High | -Add encryption and further security to data  -Store data in separate system to other internal systems  -Frequent backing up of data |

**Figure 1** – (*Likelihood & Impact scale*)

A close-up of a document

AI-generated content may be incorrect.

**Figure 2** – (*Impact calculator*)

A table with text on it

AI-generated content may be incorrect.

**Recommendations**

**To be implemented ASAP:**

-Develop organisational wide awareness and training for security (Access Control & Incident Management Risks)

-Add 2FA (Access Control Risk)

-Create Inventory list of IT Assets (Access Management Risk)

-Add Locks to server doors (Physical Security Risk)

-Limit access to authorised personnel only (Physical Security Risk)

-Frequent backing up of data (Data protection Risk)

**To be implemented within 3 months:**

-Add 2FA (Access Control Risk)

-Monitoring of who, when and where a login occurs (Access Control Risk)

-Frequent stock checks (Asset Management Risk)

-Create report system for organisation (Incident Management Risk)

-Have frequent IT staff checks and scans of organisation computers and networks for security incidents (Incident Management Risk)

-Improve Surveillance for physical security incident threats (Incident Management Risk)

-Surveillance in, on and around server rooms (Physical Security Risk)

-Add encryption and further security to data (Data Protection Risk)

-Store data in separate system to other internal systems (Data Protection Risk)

**To be implemented within 12 months:**

-Add a “Consequence Management system” for any sharing of passwords (Access Control Risk)

**Conclusion**

There is a wide array of potential threats identified, all of which provide a moderate to high risk to the organisation. As a result, these risks must be mitigated with haste due to the field of work and degree of responsibility the company holds.