4.3 Security

4.3.1 Cyber Security Risk Assessment (Summary)

A mini risk assessment was performed for Truelec's new HQ and Brisbane branch using the unit template (TVA Matrix).
It considered threats, vulnerabilities, impacts, and likelihoods across eight major information-security threats.
Assets included hardware, software, data, people, and processes; four key data assets were assessed.

Key Assets & Threats Evaluated

#	Threat Type	Vulnerability / Description	Asset Affected	Impact	Likelihood	Risk Level
1	Malware / Ransomware	Unpatched PCs or USB devices	CRM & HR Data	High	Medium	High
2	Phishing / Social Engineering	Staff may click malicious email links	Employee Credentials	High	High	High
3	Insider Threat	Disgruntled employee downloads client data	Project Files / CRM	High	Medium	High
4	Unsecured Wi-Fi Access	Weak or shared passwords on APs	HQ Wi-Fi Network	Medium	High	High
5	Data Loss / Hardware Failure	Single server point of failure	HR Records, CRM	High	Low	Medium
6	DDoS Attack on Public Website	No cloud WAF / rate-limit	Company Website	Medium	Medium	Medium
7	IoT Vulnerability	Default passwords on CCTV / RFID	IoT Feeds	Medium	Medium	Medium
8	Physical Damage / Power Loss	No UPS or backup generator	Servers & Routers	High	Low	Medium

Data Assets Considered

1. HR Employee Records (personal & payroll)
2. CRM Client Database (contact and project history)
3. Financial Accounting Data (Xero/ERP exports)
4. IoT Sensor & CCTV Footage (security feeds)

Among these, the CRM Client Database was rated Highest Risk due to its business sensitivity, exposure through remote VPN access, and susceptibility to phishing & malware.

4.3.2 Recommended Security Controls (NIST SP 800-53 Aligned)

Target Asset — CRM Client Database

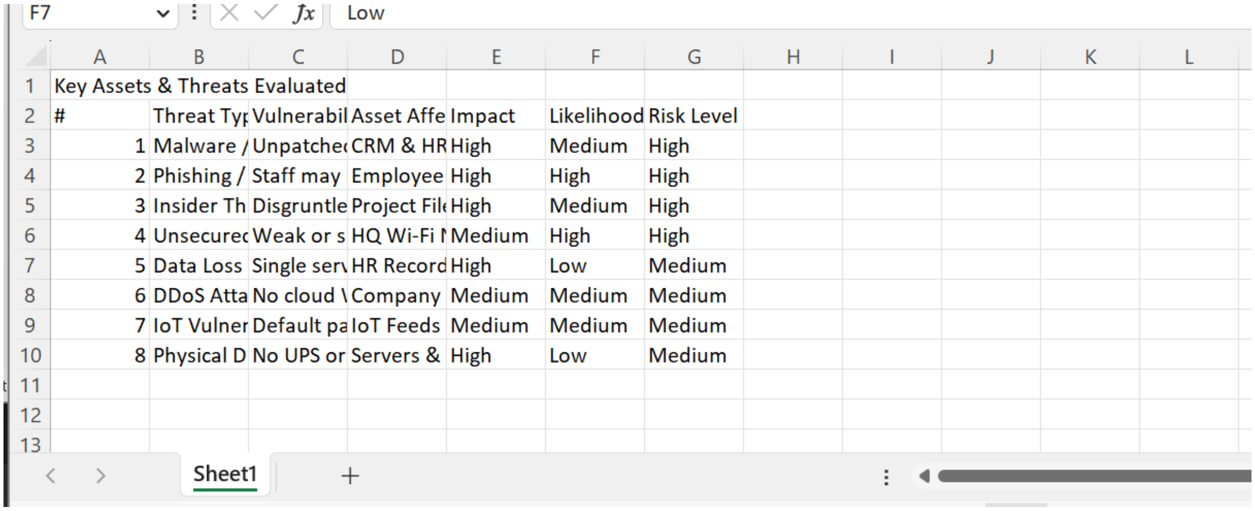
The following three controls were selected as most effective for reducing risk:

Control ID	Control Name	Implementation in Truelec	Risk Reduced	User Impact / Disadvantage
AC-2	Account Management	• Apply Role-Based Access Control (RBAC) on the CRM server. • Only authorised staff in Sales & Management groups can view client records. • Implemented via Windows AD integration on 48.12.0.0/24 (HQ Server Subnet).	Prevents unauthorised viewing or exfiltration of client data.	Users may need additional logins or approval for new access requests.
IA-2	Identification & Authentication (MFA)	• Enforce Multi-Factor Authentication for all CRM logins (software token or SMS OTP). • Applies to HQ and remote VPN users. • Configured on CRM web portal and VPN gateway (router 48.40.0.3).	Stops credential-stuffing and phished-password attacks.	Slightly slower login; requires mobile device for OTP.
SC-28	Data Encryption at Rest	• Enable AES-256 disk encryption on CRM VM and database storage volume. • Keys managed in Azure Key Vault if migrated to cloud.	Ensures stolen drives or backups cannot reveal client data.	Minor CPU overhead; admins must rotate keys securely.

Summary of Benefits

- AC-2 (RBAC): Ensures only authorised roles access CRM data.
- IA-2 (MFA): Adds a second authentication layer for remote logins.
- SC-28 (Encryption): Protects stored data if servers or backups are compromised.

Together, these controls address confidentiality, integrity, and availability (CIA triad) principles, directly lowering the highest-rated risk from High to Low–Medium.



F7 | Low

	A	B	C	D	E	F	G
1	Key Assets & Threats Evaluated						
2	#	Threat Typ	Vulnerabil	Asset Affe	Impact	Likelihood	Risk Level
3	1	Malware /	Unpatche	CRM & HR	High	Medium	High
4	2	Phishing /	Staff may	Employee	High	High	High
5	3	Insider Th	Disgruntle	Project Fil	High	Medium	High
6	4	Unsecure	Weak or s	HQ Wi-Fi N	Medium	High	High
7	5	Data Loss	Single serv	HR Record	High	Low	Medium
8	6	DDoS Atta	No cloud \	Company	Medium	Medium	Medium
9	7	IoT Vulner	Default pa	IoT Feeds	Medium	Medium	Medium
10	8	Physical D	No UPS or	Servers &	High	Low	Medium