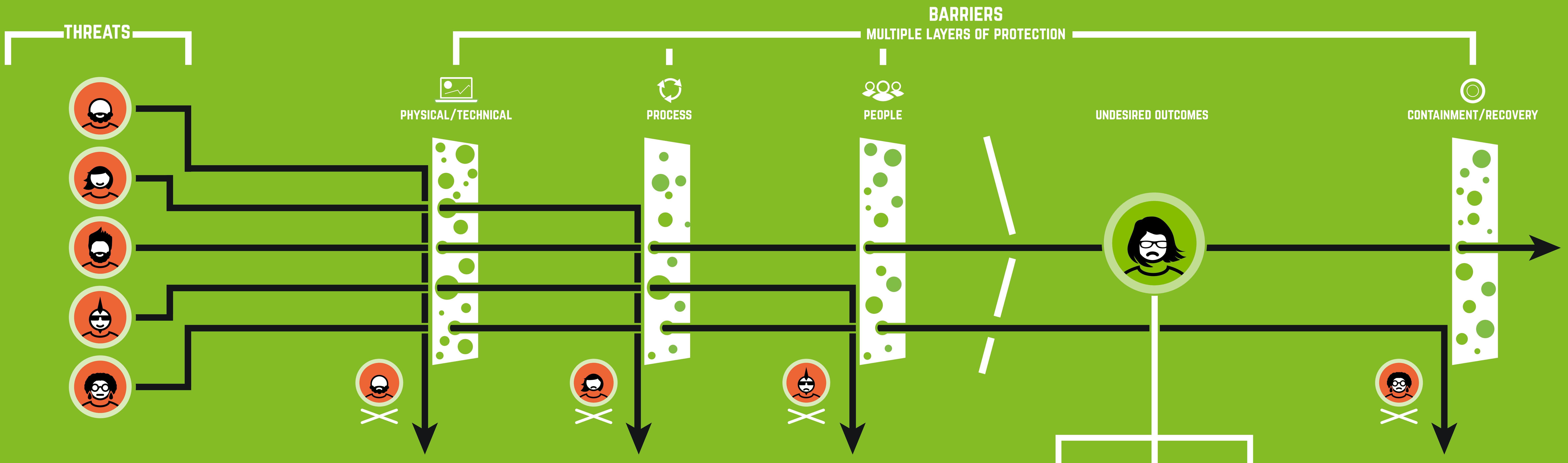
SWISS CHEESE MODEL

CLOUD COMPUTING – RISKS & MITIGATIONS ANALYSIS



THREATS

- Force Majeure
- Terrorism / Activists
- Criminal Activity / Hacking
- Utility Service Outage
- Denial of Service Attacks
- Snooping by Government Agencies
- Requests for Data by Government Agencies
- Regulatory / Legal / Legislative Change
- Civil Unrest / Pandemic / Wide Scale Industrial Action
- Data Is Intercepted in Transit
- Data Centre Hardware Failures
- Bug / Vulnerability in Infrastructure
- Cloud Provider Goes Out of Business
- Contract with Cloud Provider is Terminated
- Strategic Shift by Cloud Provider
- Bug / Vulnerability in Application Code
- Uncontrolled Usage of Resources
- Spike in Use of Services
- Enforced Upgrades
- Disgruntled Employee
- Mistake by Employee

OWNERSHIP	PHYSICAL/TECHNICAL CONTROL	PROCESS CONTROL	PEOPLE/ORGANISATIONAL CONTROL
Controls solely the responsibility of the Cloud Provider	• Choice of Data Centre Location • High Security Premises • Multiple Utility Connections (Power, Communications, Water) • Physical Infrastructure Resilient by Design • Geo Replication • Spares Carried for Key Kit • Flexible Capacity • Logical Segregation of Tenants / Subscriptions • Secure Deletion of Data No Longer in Use • Metering of Use • Monitoring Tools • Management Tools	• Preventative Maintenance of Equipment • Secure Disposal of Physical Media • Active Virus Scanning • Independent Audits • Regular Patching and Upgrades	
Controls where there is a joint responsibility between Cloud Provider and Tenant	• Secure Remote Access for Tenant Administrators • Encryption of Data at Rest • Encryption of Data in Transit • Robust Network Security (Firewalls)	• 24 X 7 Operational Monitoring • 24 X 7 Service Desk • Strict Access Control	
Controls solely the responsibility of the Tenant		• Regular Backups of Data	• Understanding of Cloud Economics • Understanding of Cloud Services and How to Apply Them Successfully
Controls implemented independently by both the Cloud Provider and the Tenant		• Change Management • Peer Review / Quality Assurance / Testing • Audit Trails / Activity Logging • Penetration Testing • Disaster Recovery Testing • Robust Architecture Processes	• Vetting of Staff • People with The Right Skills and Experience • Clear Roles and Responsibilities • Segregation of Duties • Training/Accreditation Programme • Staff Awareness of Risks • Strong Management • Adequate Resourcing Levels • Effective Communications

Information Security:
- Uncontrolled Leakage of Information
- Breach of Data Security Law

Commercial:
- Overspend
- Vendor Lock In

Performance:
- Unplanned Outages
- Poor Performance
- Insufficient Capacity

CONTAINMENT/RECOVERY CONTROL
• Local Power Generators • Selective Shut Down of Services • Major Incident Management Procedure
• Comprehensive Business Continuity Plan • Migration of Services to Other Data Centre Location
• Restoration from Backup

produced in collaboration with
HYMANS # ROBERTSON & endjin Microsoft Partner