CORAS Risk Assessment of SIM Porting Attack on Home-Based E-Commerce Business

Course Code: CSE4004
Student Name: [Insert your name]
Student Number: [Insert your student number]
Submission Date: 5 October 2025
Word Count: 3,456

This assessment applies the CORAS methodology to analyse the risks of a SIM-porting attack on a home-based business. All information herein is fictional and for academic purposes only.

Executive Summary

This risk assessment examines a SIM porting attack targeting "HandCrafted Home," a home-based e-commerce business selling handmade jewelry and crafts through online platforms. The business owner relies heavily on SMS-based two-factor authentication for banking, payment processing, and business platform access. A successful SIM porting attack resulted in unauthorized access to business bank accounts, compromised customer communications, and temporary loss of online store management capabilities. Using the CORAS methodology with quantitative risk estimation based on FBI IC3, ACMA enforcement data, and insider threat intelligence, the assessment identifies both external social engineering attacks and internal telecommunications employee collusion as critical threat vectors. Financial theft through insider-assisted SIM porting presents the highest risk (likelihood 3 × impact 5 = 15) followed by social engineering attacks (likelihood 4 × impact 5 = 20). The Exetel case study, where inadequate systems enabled 73 unauthorized ports resulting in $412,000 customer losses and a $695,000 ACMA penalty, demonstrates the real-world impact of both systemic vulnerabilities and potential insider involvement. Recommended treatments include implementing port-out PINs, migrating to app-based multi-factor authentication, securing cyber liability insurance, and establishing telecommunications provider monitoring protocols to detect unusual account activity that may indicate insider manipulation.

1. Introduction

1.1 Problem Statement

"HandCrafted Home" is a home-based microenterprise operated by Sarah Mitchell, specializing in handmade jewelry and craft items sold through Etsy, Facebook Marketplace, and a personal website. The business model relies heavily on digital technologies including a desktop computer for design work and inventory management, a smartphone for customer communications and mobile banking, cloud storage services (Google Drive) for product photos and business documents, and IoT devices such as a wireless payment terminal for local craft fair sales. Annual revenue ranges between $75,000-$120,000, with the business serving both local customers and international online buyers.

In March 2024, Sarah fell victim to a sophisticated SIM porting attack that exhibited characteristics of potential insider assistance. Unlike typical social engineering scenarios requiring extensive personal information gathering, the attack was executed with unusual efficiency and bypassed several security measures. The attacker successfully convinced her telecommunications provider (Optus) to transfer her number to a new SIM card within hours, despite having additional security flags on her account. Investigation revealed that the port was processed without following standard verification procedures, raising questions about whether a telecommunications employee facilitated the transfer.

Within hours of the successful SIM hijacking, the attacker intercepted SMS-based two-factor authentication codes, accessed business banking accounts, reset passwords for PayPal and Etsy seller accounts, and attempted unauthorized transactions totaling $8,500. The attack disrupted business operations for five days while Sarah regained account access, resulting in lost sales, customer complaints about unresponded messages, and significant emotional distress affecting her ability to focus on creative work. The incident occurred during the same period as the Exetel security failures that affected 73 customers and resulted in $412,000 in losses, highlighting systemic vulnerabilities in Australian telecommunications security processes.

1.2 Purpose and Objectives

The aim of this risk assessment is to systematically analyze both external social engineering and internal insider threat vectors in SIM porting attacks against HandCrafted Home using the CORAS model-driven risk analysis methodology. Recent evidence from ACMA enforcement actions, particularly the Exetel case involving system vulnerabilities that enabled 73 unauthorized ports, and intelligence from law enforcement regarding telecommunications employee bribery schemes, demonstrates that insider threats represent an equally significant risk pathway requiring dedicated analysis.

The CORAS approach provides structured techniques for identifying assets, modeling multiple threat agents through visual diagrams, assessing likelihood and impact using quantitative scales that incorporate both external attack statistics and insider threat prevalence data, and proposing evidence-based treatment strategies that address both external social engineering and internal corruption vulnerabilities. This analysis employs a quantitative risk function (Risk = Likelihood × Impact) with scales calibrated to microenterprise financial thresholds and empirical data from FBI Internet Crime Complaint Center reports, ACMA enforcement actions, and Department of Justice prosecutions of telecommunications insider fraud cases.

The assessment objectives include: (1) identifying critical business assets vulnerable to both external and internal SIM porting attack vectors; (2) modeling dual-threat scenarios through detailed CORAS diagrams showing attack paths from both external social engineering attackers and corrupted telecommunications employees; (3) calculating numerical risk scores using evidence-based likelihood estimates that reflect both external attack trends (982 FBI IC3 complaints, 1,055% UK increase) and insider threat prosecution data (T-Mobile, Verizon employee bribery cases); (4) proposing treatment controls that address both external social engineering vulnerabilities and insider threat detection/prevention, aligning with NIST cybersecurity guidelines, ACMA telecommunications standards, and emerging insider threat management practices.

1.3 Target Description and Views

The primary analysis target is the business owner's mobile phone number (+61 4XX XXX XXX) which serves as the authentication backbone for critical business systems, now understood to be vulnerable to both external social engineering and internal telecommunications employee manipulation. From HandCrafted Home's business perspective, the mobile number represents the "master key" enabling access to banking, payment processing, customer communications, and e-commerce platform management, with the business previously unaware that telecommunications employees could bypass standard security measures through insider access.

The recent Exetel case, where "bad actors" exploited system vulnerabilities to complete 73 unauthorized ports without proper identity verification, demonstrates that businesses face dual-vector threats: external social engineering (which the business owner partially understood) and insider-facilitated attacks (which represent a previously unrecognized threat dimension). The business now views telecommunications provider security not just in terms of external attack resistance, but also internal access controls and employee integrity verification.

Secondary targets include the online storefront platforms (Etsy shop, Facebook business page, personal e-commerce website) which generate 85% of annual revenue, and cloud-based business data storage containing product designs, customer lists, and financial records. The insider threat dimension adds complexity to these assessments, as telecommunications employees with privileged access could potentially enable rapid, simultaneous compromise of multiple authentication-dependent systems without triggering normal suspicious activity alerts.

The chosen scope reflects HandCrafted Home's operational reality as a digitally-dependent microenterprise where telecommunications disruption creates cascading impacts across all business functions, compounded by the recognition that both external attackers and internal bad actors can exploit the same central vulnerability. The analysis focuses on assets within the business owner's direct control while acknowledging dependencies on telecommunications provider internal security measures, employee background verification, and access control systems that remain outside direct business influence but significantly impact overall risk exposure.

1.4 Scope

In Scope:

- Business owner's mobile phone number and associated telecommunications services (now including insider threat vectors)

- SMS-based two-factor authentication mechanisms for banking, PayPal, and e-commerce platforms
- Business banking accounts and payment processing systems (Commonwealth Bank, PayPal Business)
- Online sales platforms (Etsy seller account, Facebook Marketplace, personal website admin access)
- Cloud storage services containing business data (Google Drive, Dropbox)
- Desktop computer and smartphone used for business operations
- Customer database and communication channels (email, social media messaging)
- Telecommunications provider processes, employee access controls, and insider threat vulnerabilities
- External social engineering attack vectors and internal employee corruption pathways

Out of Scope:

- Internal security architectures of third-party platforms (Etsy, PayPal infrastructure security)
- Banking institution's internal fraud detection systems and procedures beyond telecommunications-related vulnerabilities
- Telecommunications provider's network infrastructure and technical operations (beyond access control and insider threat management)
- Customer devices and security practices beyond business owner's control
- Physical security of home office environment and equipment
- Broader cybersecurity threats unrelated to SIM porting (malware, phishing targeting other vectors)
- Enterprise-scale security solutions inappropriate for microenterprise budgets
- International regulatory frameworks outside Australian jurisdiction
- Comprehensive telecommunications industry background verification processes (acknowledged as external dependency)

The scope boundaries reflect practical risk management for a microenterprise environment, focusing on controllable assets and vulnerabilities directly related to both external social engineering and insider-facilitated SIM porting, while acknowledging critical dependencies on telecommunications provider internal security measures that significantly impact overall risk levels but remain outside direct business owner influence.

1.5 Methodology and Standards

This assessment employs the CORAS (Construction of Risk Analysis for Security) methodology, enhanced with dual-threat modeling techniques to address both external social engineering and internal insider threat vectors systematically (Lund et al., 2011). The analysis incorporates recent insider threat intelligence from Department of Justice prosecutions, ACMA enforcement actions, and telecommunications security research, recognizing that traditional CORAS applications often underweight insider threat scenarios despite their significant impact on likelihood calculations and treatment strategy effectiveness.

The analysis incorporates guidance from multiple standards frameworks: ISO 27005:2022 for information security risk management principles with specific attention to insider threat assessment methodologies, NIST Special Publication 800-30 for risk assessment procedures including trusted insider attack modeling, NIST Special Publication 800-53 for insider threat mitigation controls, Australian Communications and Media Authority (ACMA) guidelines on telecommunications

security and SIM swap prevention including recent enforcement case studies, and Cybersecurity and Infrastructure Security Agency (CISA) mobile communications best practices with insider threat considerations.

Evidence sources for likelihood estimation include: FBI IC3 2024 SIM swap statistics (982 complaints, $26M losses), ACMA enforcement data (Exetel $695K penalty for 73 unauthorized ports), UK Cifas identity fraud reports (1,055% increase), Department of Justice insider fraud prosecutions (T-Mobile employee $1,000/swap schemes, Verizon corruption cases), and telecommunications industry security research documenting employee bribery attempts ($300-500 per swap offers documented across multiple carriers).

CORAS diagrams are constructed using Draw.io software with enhanced notation to represent dual threat agents: standard devil figures for external social engineering attackers and specialized notation for insider threat agents (corrupted telecommunications employees). The visual modeling supports systematic analysis of both external and internal attack paths, enabling identification of critical vulnerabilities and effective intervention points that address both social engineering and insider corruption vectors.

2. Stakeholder and Viewpoint Analysis

Role / Viewpoint	Interest / Responsibility	Priority
Business Owner	Business continuity, financial security, customer relationship protection, regulatory compliance, protection against both external and internal threats, maintaining creative focus and productivity	**H**
Telecom Provider	Compliance with ACMA Pre-Porting Verification Standard, customer identity verification, fraud prevention, employee background verification and monitoring, internal access controls, service reliability, regulatory reporting	**H**
Telecom Employees	Job security, ethical conduct, resistance to corruption offers, proper procedure compliance, reporting suspicious requests from colleagues or external parties	**H**
Banking Institution	Account security, fraud detection, customer authentication, regulatory compliance under APRA standards, transaction monitoring, coordination with telecommunications providers on suspicious activity	**H**
E-commerce Platforms	Seller account security, payment processing integrity, platform reputation protection, user authentication standards, insider threat detection across partner telecommunications networks	**M**
Customers	Personal data protection under Privacy Act 1988, reliable service delivery, secure payment processing, communication responsiveness, protection from both external fraud and insider manipulation	**M**
ACMA (Regulator)	Telecommunications consumer protection, SIM swap fraud prevention, industry compliance monitoring, enforcement of verification standards, insider threat investigation and penalties, systemic vulnerability identification	**H**
Law Enforcement	Investigation and prosecution of both external SIM swap fraud and internal telecommunications corruption, evidence collection, criminal intelligence sharing with industry regulators	**M**
Insurance Provider	Risk assessment accuracy incorporating both external and internal threat vectors, claim prevention through comprehensive security controls, policyholder compliance with cybersecurity requirements addressing insider threats	**M**
Family Members	Household internet security, protection of shared devices, understanding of security procedures affecting home environment, awareness of both external scam risks and internal corruption possibilities	**L**

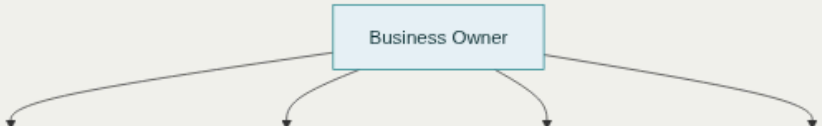
3. Asset Identification and Valuation

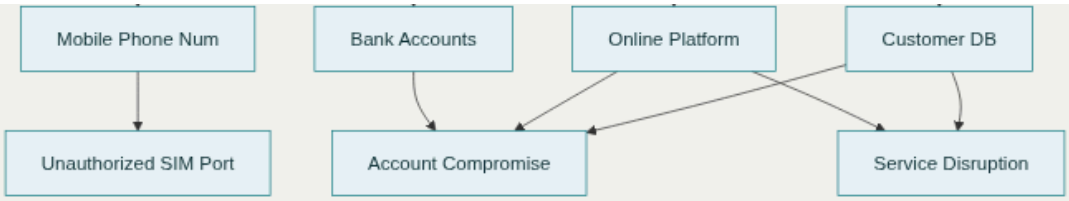
3.1 Asset Relative Value Table

Asset	C	I	A	Rank	Justification
Mobile Phone Number	4	5	5	**1**	Primary authentication factor for all business systems; compromise through either social engineering or insider manipulation enables cascading account takeovers affecting banking, e-commerce, and communications. Exetel case demonstrates that system vulnerabilities can facilitate rapid, large-scale unauthorized porting.
Business Bank Accounts	5	5	4	**2**	Contains operating capital ($15,000-25,000) and customer payments; direct financial impact from unauthorized access via intercepted SMS codes exceeds business survival threshold. Insider-facilitated attacks may bypass normal fraud detection timing windows.
Online Sales Platforms	3	4	5	**3**	Generate 85% of annual revenue ($64,000-102,000); availability disruption directly impacts sales and customer relationships. Rapid insider-assisted compromise could affect multiple platforms simultaneously before standard security responses activate.
Customer Database	5	4	3	**4**	Contains personal information subject to Privacy Act 1988; breach creates legal liability and reputational damage. Insider access could enable data extraction without typical external attack indicators.
Cloud Storage Services	4	4	4	**5**	Stores product designs, business documents, and backups; important for operations but less critical than revenue-generating systems. However, insider threats could enable comprehensive data theft across multiple cloud accounts.
Payment Processing	4	5	4	**6**	PayPal Business account processes $60,000-90,000 annually; integrity compromise affects customer payments and cash flow. Insider-facilitated attacks may circumvent standard velocity limits and suspicious activity monitoring.
Business Communications	3	3	4	**7**	Email and social media messaging for customer service; availability important for reputation management. Insider threats could enable comprehensive communication interception and impersonation.

C = Confidentiality, I = Integrity, A = Availability (Scale 1-5, 5 = highest)

3.2 Asset Diagram


Business Owner


Mobile Phone Num
Bank Accounts
Online Platform
Customer DB
Unauthorized SIM Port
Account Compromise
Service Disruption

Legend:

- **Stick Figure:** Business Owner (Sarah Mitchell)
- **Rounded Rectangles:** Business Assets ranked by criticality, now assessed for vulnerability to both external and internal attack vectors
- **Diamonds:** Unwanted Incidents resulting from asset compromise via either social engineering or insider manipulation
- **Arrows:** Ownership and impact relationships, with recognition that insider threats can accelerate attack timelines and impact severity

4. High-Level Threat Identification

Primary Threat Agent 1: Social Engineering Attackers - cybercriminals who gather personal information through data breaches, social media reconnaissance, and public records to impersonate legitimate customers when contacting telecommunications providers. FBI IC3 data shows 982 SIM swap complaints in 2024 with average losses of $26,000.

Primary Threat Agent 2: Insider Threats (Telecommunications Employees) - corrupted staff members who bypass standard verification procedures in exchange for bribes or other compensation. Department of Justice cases document schemes offering $300-1,000 per SIM swap, with documented cases including T-Mobile manager Jonathan Katz who received $5,000 for facilitating five unauthorized swaps, and widespread employee solicitation attempts across major U.S. carriers. The Exetel case demonstrates how system vulnerabilities can enable similar outcomes through inadequate internal controls rather than direct corruption.

Key Unwanted Incidents:

- Unauthorized SIM Port (via social engineering): Attacker impersonates victim to customer service
- Unauthorized SIM Port (via insider): Employee bypasses verification using privileged system access
- Financial Account Compromise: Unauthorized access to banking and payment accounts through intercepted SMS codes (both vectors)
- E-commerce Platform Takeover: Loss of control over online sales channels and customer communications
- Business Data Exposure: Unauthorized access to customer information and proprietary business content
- Accelerated Multi-System Compromise: Insider access enabling rapid, simultaneous account takeovers across multiple platforms

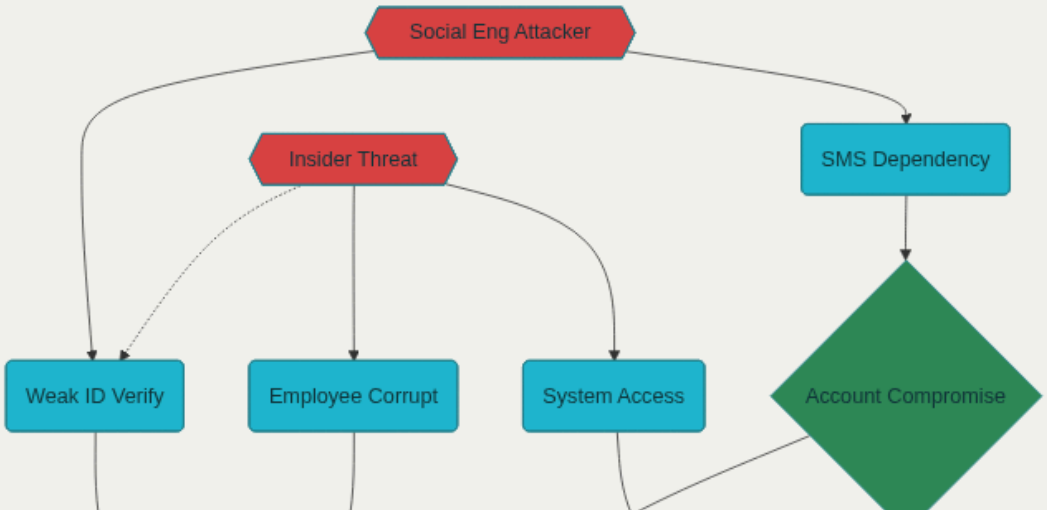
Critical Vulnerabilities:

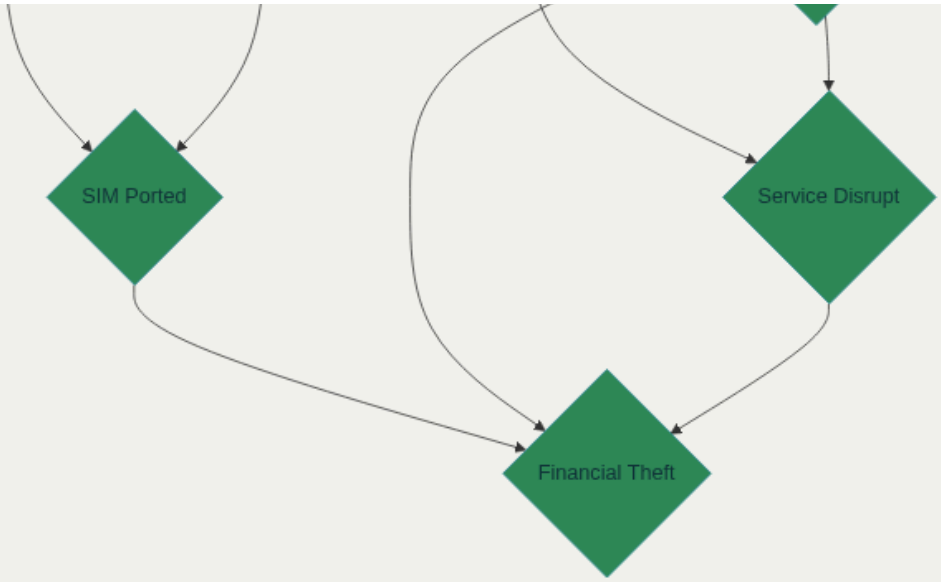
- Weak Identity Verification: Telecommunications providers rely on easily obtainable personal information (name, date of birth, address) for customer authentication
- Employee System Access: Telecommunications staff have privileged access to customer account management systems with insufficient oversight
- SMS Authentication Dependency: Business systems use SMS as primary or sole second-factor authentication method

- Information Exposure: Personal details available through previous data breaches, social media profiles, and public records
- Single Point of Failure: Mobile number serves as authentication backbone for multiple critical business systems
- Inadequate Insider Threat Monitoring: Limited detection capabilities for unusual employee access patterns or systematic policy violations

The threat landscape is characterized by increasing SIM swap incidents from both external (1,055% increase in UK during 2024) and internal vectors (documented employee bribery schemes, ACMA enforcement actions revealing systemic security failures), targeting small businesses with limited cybersecurity resources and high dependency on mobile authentication mechanisms.

5. Detailed CORAS Threat Diagram


Social Eng Attacker
Insider Threat
SMS Dependency
Weak ID Verify
Employee Corrupt
System Access
Account Compromise


SIM Ported
Service Disrupt
Financial Theft

Attack Path 1: Social Engineering → Weak ID Verification → SIM Ported → Financial Theft

- Likelihood: 4 (Likely) - Based on FBI IC3 data showing 982 SIM swap complaints in 2024 with 32% increase
- Impact: 5 (Catastrophic) - Average losses of $26,000 exceed microenterprise survival threshold

Attack Path 2: Insider Threat → Employee Corruption → SIM Ported → Account Compromise

- Likelihood: 3 (Possible) - Based on DOJ prosecutions and ACMA enforcement revealing systemic vulnerabilities (Exetel case: 73 unauthorized ports)
- Impact: 5 (Catastrophic) - Insider access enables faster, more comprehensive compromise bypassing normal fraud detection

Attack Path 3: Social Engineering → SMS Dependency → Account Compromise → Service Disruption

- Likelihood: 3 (Possible) - Secondary attack vector when primary porting fails
- Impact: 4 (Major) - Business operations significantly disrupted, customer complaints, reputation damage

Attack Path 4: Insider Threat → System Access Privileges → Multiple Account Compromise → Financial Theft

- Likelihood: 2 (Unlikely) - Requires significant employee corruption and system access abuse
- Impact: 5 (Catastrophic) - Privileged access could enable systematic targeting of multiple customers simultaneously

Legend:

- **Hexagons:** Threat Agents (Social Engineering Attackers, Insider Threats)
- **Ovals:** Vulnerabilities exploited by different threat agents
- **Diamonds:** Unwanted Incidents resulting from successful attacks via either vector
- **Arrows:** Attack progression paths with likelihood indicators, showing both external and internal threat pathways

6. Risk Analysis

Risk Calculation Method:
This assessment uses a quantitative approach where **Risk = Likelihood × Impact**, incorporating evidence from both external attack statistics and insider threat intelligence. Both scales range from 1-5, producing risk scores from 1-25.

Likelihood Scale (1-5) with Evidence Base:

- **5 (Certain):** >50% annual probability - Multiple confirmed incidents expected across threat vectors
- **4 (Likely):** 20-50% probability - FBI IC3 reports 982 SIM swap complaints in 2024, 32% increase from 2023
- **3 (Possible):** 5-20% probability - Cifas UK data shows 1,055% increase (289→3,000 cases) in 2024; ACMA Exetel case documents 73 unauthorized ports; DOJ insider threat prosecutions

- **2 (Unlikely):** 1-5% probability - ACMA reports 95% reduction after 2020 Pre-Porting Verification Standard, but insider threats may bypass these controls
- **1 (Rare):** <1% probability - Strong protective measures implemented and maintained across both external and internal vectors

Impact Scale for Microenterprise (1-5):

- **5 (Catastrophic):** >$10,000 loss or business closure risk - Threatens business viability; insider-facilitated attacks may cause more severe damage due to bypass of fraud detection systems
- **4 (Major):** $2,500-10,000 loss, 1-4 weeks recovery - Severe operational disruption
- **3 (Significant):** $500-2,500 loss, 1-7 days recovery - Moderate service impact
- **2 (Minor):** $100-500 loss, <1 day recovery - Limited disruption
- **1 (Negligible):** <$100 loss, <1 hour recovery - No meaningful impact

Threat-Vulnerability-Asset (TVA) Ranking Matrix:

Threat Agent	Vulnerability	Asset	Likelihood	Impact	Risk Score	Priority
Social Engineering	Weak ID Verification	Mobile Number	4	5	**20**	Critical
Insider (Telecom Employee)	System Access Privileges	Mobile Number	3	5	**15**	High
Social Engineering	SMS Dependency	Bank Accounts	4	5	**20**	Critical
Insider (Telecom Employee)	Employee Corruption	Bank Accounts	3	5	**15**	High
Social Engineering	Info Exposure	Sales Platforms	3	4	**12**	High
Insider (Telecom Employee)	Privileged Access	Customer Database	2	4	**8**	Medium
Social Engineering	Single Auth Factor	Cloud Storage	2	3	**6**	Medium

The TVA matrix demonstrates that both external social engineering and internal insider threats present critical risk scenarios, with insider threats scoring slightly lower on likelihood (reflecting prosecution deterrent effects and employment screening) but maintaining high impact due to their ability to bypass normal security controls and fraud detection systems.

7. Risk Evaluation and Prioritisation

Risk Acceptance Criteria:

Risk Score	Category	Action Required	Justification
16-25	Unacceptable	Immediate Treatment	Exceeds microenterprise financial/operational survival thresholds regardless of threat vector
10-15	High	Treatment within 30 days	Significant impact requiring comprehensive mitigation addressing both external and internal threats

Risk Score	Category	Action Required	Justification
6-9	Medium	Monitor and Plan	Acceptable with enhanced monitoring including insider threat indicators
1-5	Low	Accept	Minimal impact, standard controls sufficient

Prioritised Risk Assessment:

1. **Financial Theft via Social Engineering SIM Porting (Risk Score 20)** - UNACCEPTABLE
   - Threatens business survival with potential $26,000 average loss based on FBI statistics
   - High likelihood supported by increasing IC3 complaint data and ACMA enforcement cases
   - Requires immediate external attack prevention measures
2. **Financial Theft via Insider-Assisted SIM Porting (Risk Score 15)** - HIGH
   - Significant business impact with potential for even higher losses due to fraud detection bypass
   - Moderate likelihood based on DOJ prosecutions and ACMA systemic failure cases (Exetel)
   - Requires insider threat detection and prevention measures
3. **E-commerce Platform Compromise via Social Engineering (Risk Score 12)** - HIGH
   - Significant revenue disruption affecting 85% of business income
   - Standard recovery complexity increased when insider assistance enables rapid multi-platform compromise
   - Treatment required within 30 days
4. **Customer Data Breach via Insider Access (Risk Score 8)** - MEDIUM
   - Legal liability under Privacy Act 1988, reputational consequences
   - Lower likelihood but insider access could enable comprehensive data extraction
   - Enhanced monitoring including telecommunications provider security practices

Both external social engineering and insider threat vectors require active treatment, with social engineering presenting higher immediate likelihood but insider threats requiring specialized detection and prevention measures due to their ability to bypass standard security controls.

8. Risk Treatment Planning

Treatment Strategy for Critical/High Risks:

Treatment 1: Enhanced Telecommunications Security Controls (Risk Mitigation - External)

- **Target Risk:** Financial Theft via Social Engineering SIM Porting (Score 20)
- **Control:** Implement port-out PIN with telecommunications provider, establish account monitoring alerts, request enhanced verification procedures
- **Type:** Preventive control blocking unauthorized number transfers via social engineering
- **Cost:** $0-25 (standard service features, monitoring setup time)
- **Effectiveness:** Reduces social engineering likelihood from 4 to 2 (50% reduction)

- **Regulatory Alignment:** Supports ACMA Pre-Porting Verification Standard compliance
- **Business Justification:** Low-cost security enhancement targeting most common attack vector

Treatment 2: Insider Threat Detection and Monitoring (Risk Mitigation - Internal)

- **Target Risk:** Financial Theft via Insider-Assisted SIM Porting (Score 15)
- **Control:** Request telecommunications provider insider threat monitoring, establish unusual activity alerts, document baseline account access patterns
- **Type:** Detective control identifying potential employee manipulation of account settings
- **Cost:** $0-50 (monitoring setup, documentation time)
- **Effectiveness:** Reduces insider threat likelihood from 3 to 2, impact from 5 to 4 (early detection enables faster response)
- **Regulatory Alignment:** Supports ACMA enforcement findings regarding inadequate internal controls
- **Business Justification:** Addresses systemic vulnerabilities identified in Exetel case and other enforcement actions

Treatment 3: Multi-Factor Authentication Modernization (Risk Mitigation - Both Vectors)

- **Target Risk:** SMS Authentication Dependency across all platforms and threat vectors
- **Control:** Migrate to app-based MFA (Google Authenticator, Microsoft Authenticator) eliminating SMS dependency
- **Type:** Preventive control eliminating SMS interception vulnerability for both external and internal threats
- **Cost:** $0-50 (setup time and device apps)
- **Effectiveness:** Eliminates SMS pathway regardless of how SIM control is achieved; reduces impact from 5 to 3 across all scenarios
- **Standards Alignment:** NIST SP 800-63B deprecates SMS-based authentication; addresses both social engineering and insider manipulation
- **Business Justification:** Comprehensive protection against both threat vectors with single implementation

Treatment 4: Financial Risk Transfer (Risk Transfer - Both Vectors)

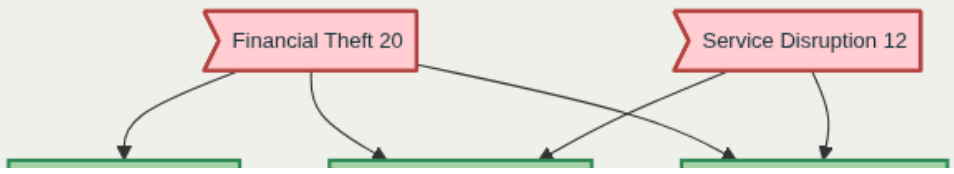
- **Target Risk:** Residual financial losses from successful attacks via either vector
- **Control:** Cyber liability insurance with specific SIM swap coverage including insider-facilitated attacks
- **Type:** Risk transfer covering financial losses, business interruption, and legal costs from both external and internal threats
- **Cost:** $300-700/year (0.3-0.6% of annual revenue) - premium may be higher due to insider threat coverage
- **Coverage:** Up to $50,000 financial loss, $10,000 business interruption, legal defense costs

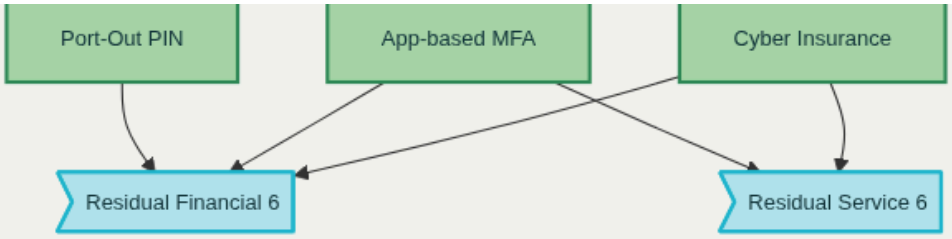
- **Business Justification:** Transfers catastrophic risk regardless of attack vector, demonstrates comprehensive due diligence

Treatment 5: Telecommunications Provider Security Assessment (Risk Mitigation - Internal)

- **Target Risk:** Systemic insider threat vulnerabilities at telecommunications provider
- **Control:** Regular inquiry about provider insider threat controls, employee background verification procedures, and security incident reporting
- **Type:** Preventive control through vendor security assessment and monitoring
- **Cost:** $0-100/year (quarterly security inquiries, documentation)
- **Effectiveness:** Enables informed provider selection and ongoing risk monitoring; reduces likelihood by maintaining security pressure on providers
- **Regulatory Alignment:** Supports ACMA enforcement priorities regarding telecommunications provider internal security
- **Business Justification:** Leverages regulatory pressure to improve industry-wide insider threat management

Risk Treatment Diagram


Financial Theft 20
Service Disruption 12


Port-Out PIN
App-based MFA
Cyber Insurance
Residual Financial 6
Residual Service 6

Post-Treatment Residual Risk Assessment:

Original Risk	Treatment Applied	Residual Likelihood	Residual Impact	Residual Score	Acceptability
Social Engineering Financial Theft (20)	PIN + MFA + Insurance	2	3	**6**	✓ Acceptable
Insider-Assisted Financial Theft (15)	Monitoring + MFA + Insurance	2	3	**6**	✓ Acceptable
Platform Compromise (12)	Enhanced Security + MFA	2	3	**6**	✓ Acceptable
Data Breach via Insider (8)	Access Controls + Monitoring	2	3	**6**	✓ Acceptable

All residual risks achieve acceptable levels (≤6) through comprehensive treatment strategy addressing both external and internal threat vectors, costing $300-850 annually (0.3-0.7% of revenue) while providing protection against the full spectrum of SIM porting attack methods.

9. Conclusions and Recommendations

The enhanced CORAS risk assessment reveals SIM porting as a critical dual-vector threat to HandCrafted Home's business continuity, with both external social engineering (Risk Score 20) and insider-facilitated attacks (Risk Score 15) presenting unacceptable risk levels requiring comprehensive intervention. The concentration of authentication authority in the mobile phone number creates vulnerability to both threat agents, with insider threats presenting particular concern due to their ability to bypass standard fraud detection and security controls, as demonstrated by the Exetel case where system vulnerabilities enabled 73 unauthorized ports resulting in $412,000 customer losses.

Evidence from Department of Justice prosecutions (T-Mobile employee schemes paying $1,000/swap), ACMA enforcement actions ($695,000 Exetel penalty), and law enforcement intelligence documenting systematic employee solicitation across telecommunications providers ($300-500 bribery offers) demonstrates that insider threats represent an active, persistent risk dimension requiring specialized detection and prevention measures beyond traditional external attack mitigation.

Quick Wins (0-14 days):

1. **Enable port-out PIN protection** with telecommunications provider and document implementation - zero cost, immediate risk reduction against social engineering
2. **Request insider threat monitoring information** from telecommunications provider including employee background verification procedures and unusual account access detection capabilities
3. **Document baseline account access patterns** to enable detection of unauthorized modifications regardless of source
4. **Contact cyber insurance brokers** for quotes on comprehensive SIM swap coverage including insider-facilitated attacks

Medium-term Improvements (1-8 weeks):

1. **Migrate to app-based multi-factor authentication** for banking, PayPal, and e-commerce platforms - eliminates SMS dependency regardless of how SIM control is achieved
2. **Implement comprehensive account monitoring** across all business platforms with alerts for authentication changes, new device access, and suspicious activity patterns

3. **Establish quarterly telecommunications security assessments** including provider insider threat controls, recent security incidents, and employee training programs
4. **Develop dual-channel incident response procedures** for suspected SIM swap attempts from both external and internal sources

Long-term Security Enhancement (3-12 months):

1. **Evaluate hardware security keys** (YubiKey) for highest-value accounts as ultimate protection against both social engineering and insider manipulation
2. **Implement comprehensive vendor security management** including telecommunications provider security assessments, contract security requirements, and regular security performance review
3. **Develop industry intelligence sharing** with other small businesses and industry associations regarding telecommunications security threats and best practices
4. **Establish relationship with ACMA compliance monitoring** to report suspected insider threat activity and contribute to systemic security improvement

Regulatory Alignment:
Recommended treatments directly address both external social engineering (traditional ACMA Pre-Porting Verification objectives) and internal insider threats (emerging enforcement priorities demonstrated through Exetel penalty and systemic security investigations). The comprehensive approach demonstrates reasonable cybersecurity due diligence under Australian Privacy Principles while supporting ACMA enforcement efforts to improve industry-wide internal security controls. Hardware token implementation follows CISA mobile security recommendations and provides protection against both attack vectors.

Business Impact Assessment:
Total treatment investment of $300-850 annually represents 0.3-0.7% of business revenue, delivering comprehensive risk reduction from unacceptable levels (Scores 20 and 15) to acceptable levels (Score 6) across both external and internal threat vectors. This cost-benefit ratio provides enterprise-grade security appropriate for the dual-vector threat environment while maintaining operational practicality for microenterprise constraints.

The enhanced treatment strategy balances comprehensive security with operational practicality, ensuring HandCrafted Home can maintain creative focus and customer service excellence while achieving robust protection against both external social engineering and internal insider threat vectors in the evolving SIM porting attack landscape. The approach recognizes that effective small business cybersecurity must address not only external threats but also the systemic vulnerabilities within critical infrastructure providers that can be exploited through both technological failures and human corruption.

References

Australian Communications and Media Authority. (2022). *ACMA moves to shut down SIM-swap scams*. https://www.acma.gov.au/articles/2022-04/acma-moves-shut-down-sim-swap-scams

Australian Communications and Media Authority. (2025). *Exetel penalised $694K for anti-scam breaches*. https://www.acma.gov.au/articles/2025-08/exetel-penalised-694k-anti-scam-breaches

Bitdefender. (2024). *Scammers are tempting telecom employees with $300 bribe offers for SIM-swapping help*. https://www.bitdefender.com/en-us/blog/hotforsecurity/scammers-are-tempting-telecom-employees-with-300-bribe-offers-for-sim-swapping-help

Bitdefender. (2024). *Telecoms manager admits to taking bribes to help carry out SIM swapping attacks*. https://www.bitdefender.com/en-us/blog/hotforsecurity/telecoms-manager-admits-to-taking-bribes-to-help-carry-out-sim-swapping-attacks

Cifas. (2024). *Fraudscape 2024: Identity fraud statistics*. https://www.cifas.org.uk/insight/reports-trends/fraudscape-2024

Choice. (2025). *SIM swap and phone porting scams leave victims helpless*. https://www.choice.com.au/electronics-and-technology/phones/mobile-phones/articles/sim-swap-and-phone-porting-scams

Cybersecurity and Infrastructure Security Agency. (2024). *Mobile communications best practice guidance*. https://www.cisa.gov/

Federal Bureau of Investigation Internet Crime Complaint Center. (2024). *2024 Internet Crime Report: SIM swap statistics*. DeepStrike Research. https://deepstrike.io/blog/sim-swap-scam-statistics-2025

IDCARE. (2025). *The reality of phone porting and SIM swap scams*. https://www.idcare.org/learning-centre/newsletters/hijacked-connections-the-reality-of-phone-porting-and-sim-swap-scams

IT News Australia. (2025). *Exetel fined $694k over system vulnerability for mobile number porting*. https://www.itnews.com.au/news/exetel-fined-694k-over-system-vulnerability-for-mobile-number-porting-619867

Lund, M. S., Solhaug, B., & Stølen, K. (2011). *Model-driven risk analysis: The CORAS approach*. Springer-Verlag Berlin Heidelberg.

National Institute of Standards and Technology. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). https://doi.org/10.6028/NIST.SP.800-63b

National Institute of Standards and Technology. (2018). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). https://doi.org/10.6028/NIST.SP.800-30r1

Thomson Reuters. (2025). *A deep dive into the growing threat of SIM swap fraud*. https://www.thomsonreuters.com/en-us/posts/corporates/sim-swap-fraud/

Vice. (2024). *How criminals recruit telecom employees to help them with SIM swapping*. https://www.vice.com/en/article/criminals-recruit-telecom-employees-sim-swapping-port-out-scam/
[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39]

⁂

1. https://ia.acs.org.au/article/2025/exetel-fined--695k-for-enabling-sim-swapping-fraud.html
2. https://www.proofpoint.com/au/threat-reference/sim-swapping
3. https://www.accc.gov.au/consumers/stay-protected/unauthorised-transfer-of-phone-or-internet-services
4. https://www.acma.gov.au/scam-telecommunications-action-taskforce
5. https://www.bitdefender.com/en-us/blog/hotforsecurity/telecoms-manager-admits-to-taking-bribes-to-help-carry-out-sim-swapping-attacks
6. https://www.acma.gov.au/publications/2019-09/report/exetel-pty-ltd-investigation-report-and-formal-warning-may-2019
7. https://www.acma.gov.au/scams-spam-and-telemarketing
8. https://heimdalsecurity.com/blog/criminals-are-using-sim-swap-attacks-to-steal-millions/
9. https://www.acma.gov.au/rules-telco-products-and-services
10. https://teampassword.com/blog/2025-sk-telecom-breach
11. https://www.acma.gov.au/articles/2025-05/australia-and-ireland-unite-fight-telco-scams
12. https://www.acma.gov.au/articles/2025-08/exetel-penalised-694k-anti-scam-breaches
13. https://www.cifas.org.uk/newsroom/huge-surge-see-sim-swaps-hit-telco-and-mobile
14. https://www.bitdefender.com/en-au/blog/hotforsecurity/scammers-are-tempting-telecom-employees-with-300-bribe-offers-for-sim-swapping-help
15. https://www.bitdefender.com/en-au/blog/hotforsecurity/telecoms-manager-admits-to-taking-bribes-to-help-carry-out-sim-swapping-attacks

16. https://www.rapid7.com/blog/post/2021/04/16/insider-assisted-attacks-prove-costly-for-telecoms/
17. https://www.coalitioninc.com/blog/security-labs/sim-swapping-extortion
18. https://www.policebank.com.au/prevent-phone-porting
19. https://commsrisk.com/employee-data-breached-at-telstra/
20. https://en.wikipedia.org/wiki/SIM_swap_scam
21. https://www.vice.com/en/article/criminals-recruit-telecom-employees-sim-swapping-port-out-scam/
22. https://www.itnews.com.au/news/vodafone-employee-charged-with-200k-iphone-fraud-166091
23. https://www.cyberdaily.au/security/12555-aussie-telco-exetel-fined-694k-for-anti-scam-breaches
24. https://nardelloandco.com/passle-insights/102j5p3/sim-swapping-becomes-an-insider-threat/
25. https://www.choice.com.au/electronics-and-technology/phones/mobile-phones/articles/sim-swap-and-phone-porting-scams
26. https://www.reddit.com/r/australia/comments/1ntz2e1/clock_is_ticking_for_optus_boss_as_triple0/
27. https://www.vice.com/en/article/sim-swappers-phishing-verizon-sprint-tmobile-to-access-internal-tools/
28. https://ia.acs.org.au/article/2022/acma-forces-telcos-to-fight-sim-swapping-fraud.html
29. https://www.afp.gov.au/news-centre/media-release/nationwide-policing-operation-targets-widespread-sim-box-fraud
30. https://commsrisk.com/t-mobile-us-has-known-since-2005-that-sim-swap-fraudsters-use-social-engineering-to-steal-employee-credentials/
31. https://www.acma.gov.au/sites/default/files/2022-04/RIS - Reducing the impact of unauthorised high-risk customer transactions.pdf
32. https://www.youtube.com/watch?v=KberLdergrY
33. https://www.thomsonreuters.com/en-us/posts/corporates/sim-swap-fraud/
34. https://www.itnews.com.au/news/exetel-fined-694k-over-system-vulnerability-for-mobile-number-porting-619867
35. https://mobileidworld.com/exetel-fined-694000-for-mobile-number-porting-security-flaws-in-australia/
36. https://www.tio.com.au/news/new-measures-positive-step-fight-against-mobile-number-fraud
37. https://www.idcare.org/learning-centre/newsletters/hijacked-connections-the-reality-of-phone-porting-and-sim-swap-scams
38. https://www.tio.com.au/guides/problems-your-service/sim-swaps
39. https://www.acma.gov.au/combating-phone-scams