SETU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

M.Sc Cybersecurity, Privacy & Trust

Student: **Declan Clune**
Supervisor: **Mr. Paul Barry**

DISSERTATION PROJECT

How can Cyber Threat Intelligence Address 'Harvest Now, Decrypt Later' Risk in Financial Services?

RESEARCH OVERVIEW

BACKGROUND

Quantum computing threatens the encryption that protects our most sensitive data. Adversaries can capture encrypted information today and decrypt it in the future when quantum capabilities mature – a risk known as **Harvest Now, Decrypt Later** (HNDL). Financial Services are particularly exposed due to long data retention, high-value information and strict regulatory requirements.

RESEARCH AIM

To explore how **Cyber Threat Intelligence (CTI)** can support better decision-making in preparing for and mitigating the long-term risk of **Harvest Now, Decrypt Later** (HNDL) in financial services.

RESEARCH QUESTIONS

PRIMARY QUESTION

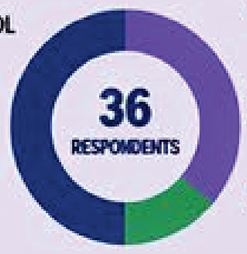
How can Cyber Threat Intelligence support decision-making to mitigate 'Harvest Now, Decrypt Later' risk in financial services?

SECONDARY QUESTIONS

- How is HNDL conceptualised in existing literature?
- What characteristics of financial services amplify HNDL risk?
- Do existing CTI models adequately address long-term cryptographic threats?

METHODOLOGY

- **Literature Review** – CTI, Quantum Risk & HNDL
- **Questionnaire** – 36 Cybersecurity & Risk Professionals
- **Thematic Analysis** – Identified key patterns and insights



47% Cybersecurity Practitioners
31% Risk & Compliance Professionals
22% Other (IT, Audit, Consulting)

KEY FINDINGS

AWARENESS IS EMERGING
HNDL is known but not yet a priority for most organisations.

CTI FOCUSES ON THE SHORT TERM
Used primarily for immediate and operational threats.

LONG-TERM RISK IS OVERLOOKED
Limited integration of future threats like quantum computing.

HIGH EXPOSURE, LOW PREPAREDNESS
Financial services are vulnerable but not yet ready.

KEY INSIGHT
There is a clear mismatch between what CTI currently does (short-term threat detection) and what HNDL requires (long-term strategic risk planning).

FRAMEWORK & CONTRIBUTION

CURRENT CTI LANDSCAPE

Mature CTI platforms provide powerful capabilities, but they are primarily designed for immediate threats. This research shows how they can be extended to address long-term cryptographic risk.

MISP Threat Intelligence
SHARE & MANAGE THREAT INDICATORS
Open-source platform that enables collaborative intelligence sharing and standardised indicator management.

OPENCTI
MODEL THREAT RELATIONSHIPS
Maps connections between actors, campaigns, TTPs and MITRE ATT&CK techniques for deeper strategic insight.

ANOMALI
PRIORITISE & AUTOMATE DECISION SUPPORT
Enterprise platform that aggregates threat data, applies prioritisation and supports decision-making at scale.

PROPOSED FRAMEWORK: CTI FOR HNDL

01 INTELLIGENCE COLLECTION
- Threat Feeds & Dark Web
- Shared Intelligence (**MISP**)
- Commercial & Proprietary Feeds (Anomali)
- Internal Security Telemetry

02 INTELLIGENCE PROCESSING & ENRICHMENT
- Indicator Management (**MISP**)
- Relationship & Context Mapping (**OpenCTI**)
- Data Aggregation, Prioritisation & Automation (**Anomali**)

03 TEMPORAL RISK ANALYSIS (NEW CONTRIBUTION)
- Short-Term Threats (Active Attacks)
- Medium-Term Threats (Emerging Capabilities)
- Long-Term Threats (**HNDL / Quantum Risk**)
- Data Sensitivity & Lifespan Tracking
- Cryptographic Exposure Analysis

04 DECISION-MAKING SUPPORT
- Operational: Incident Response
- Tactical: Risk Mitigation
- Strategic: Post-Quantum Cryptography Transition & Crypto-Agility Planning

05 ORGANISATIONAL OUTCOMES
- Improved Resilience
- Future-Proof Encryption Strategies
- Better Long-Term Planning
- Reduced Future Data Exposure

KEY CONTRIBUTION TO KNOWLEDGE

- Demonstrates that CTI must evolve beyond short-term threats
- Introduces a temporal dimension to threat intelligence
- Shows how **MISP, OpenCTI** and **Anomali** can support long-term cryptographic risk
- Provides practical recommendations for Financial Services

RECOMMENDATIONS

- Introduce **Time-Based Intelligence Classification** (Short, Medium, Long Term)
- Enhance CTI Platforms with **Cryptographic Risk Metadata**
- Integrate **Quantum Threat Intelligence Feeds**
- Align CTI Outputs with **Strategic Decision-Making**

KEY TAKEAWAY

CTI is not just about understanding today's threats – it **must evolve** to help organisations **prepare for threats that have not yet materialised.**