Information & Knowledge Leakage: An Organizational Perspective

Carlos A. Agudelo

cagudelo@student.unimelb.edu.au

@agudeloandres

Supervisors:
Dr. Rachelle Bosua
Dr. Atif Ahmad
Dr. Sean B. Maynard

THE UNIVERSITY OF MELBOURNE


DANGER

Are The Equifax, SEC And Deloitte Cybersecurity Breaches Desensitizing Society To This Threat?

Melissa Agnes, CONTRIBUTOR

Helping organizations becom

Opinions e

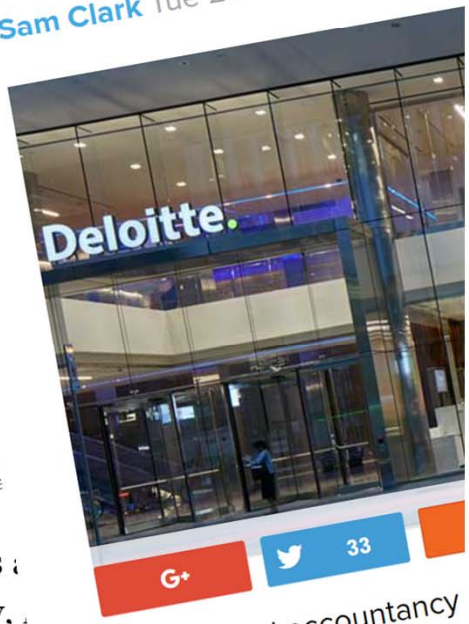
Photographer: Michael Nagle/Bloombe

Every organization has
that are the most likely,

SECURITY

Deloitte cyberattack leaks emails and details of clients

Sam Clark Tue 26 Sep 2017 11.30a



Major global accountancy
ulting in th

NEWS

US Securities and Exchange Commission discloses it was hacked last year

By Riddhi Mukherjee (@me_myslr riddhi@medianama.com) September 22, 2017

Share This: Share via Email

Two weeks after international credit rating agency Equifax revealed that it had experienced a

Outline

1. Motivation
2. Definitions:
    1. Knowledge Leakage
    2. Knowledge Leakage Risk
    3. Knowledge Contexts
3. Knowledge Leakage Framework
4. Methodology
5. Preliminary Findings
6. Contributions
7. Limitations & Future work

Motivation

THE UNIVERSITY OF MELBOURNE

- As part of the **knowledge economy**, Australian organizations are driving innovation and leveraging technology to generate products and services based on **knowledge-intensive** activities.
- Knowledge-Intensive Organizations rely on the **intellectual capabilities** of their employees (**Knowledge-workers**)-Human capital.
- The use of **mobile technologies and social media** (cloud computing, social network and smart devices) has become essential to **knowledge-workers** as they provide everyday communication, access to email, internet, working from home, airport , hotels, etc.

Knowledge Intensive Firm (KIF)

- Knowledge-Intensive Firm or Knowledge-based organization:

  are characterized by an analytical knowledge base and there is a strong reliance on knowledge as a basis for competitive advantage.

  KIF are distinguished from other kinds of firms in that they are said to contain unique qualities; they claim to produce qualified products and/or service, and even generate new and unique knowledge.

  Anand, Gardner, & Morris, 2007; Teece, 2003; Winch & Schneider, 1993)

Motivation (cont.)

THE UNIVERSITY OF MELBOURNE

- However mobile devices have also **increased** the organizational risks and impacted the risk profile of Australian Organizations opening the door to **leakage** of Intellectual property, trade secrets, designs (organizational knowledge) – Challenging **organizational boundaries**
- Each security incident in **Australian** business cost an average **US$2.8 million**.
- Australian organisations spend the **second most worldwide** (US$1.2 million each on average) investigating and assessing these breaches.
- Employees whether **deliberately** or **inadvertently** are usually more responsible than hackers for the leakage of knowledge – **insider threat**.
- **Culture and People** within an organisation are just as likely to be the source of leakage – **People** are the new **perimeter** (weakest link)

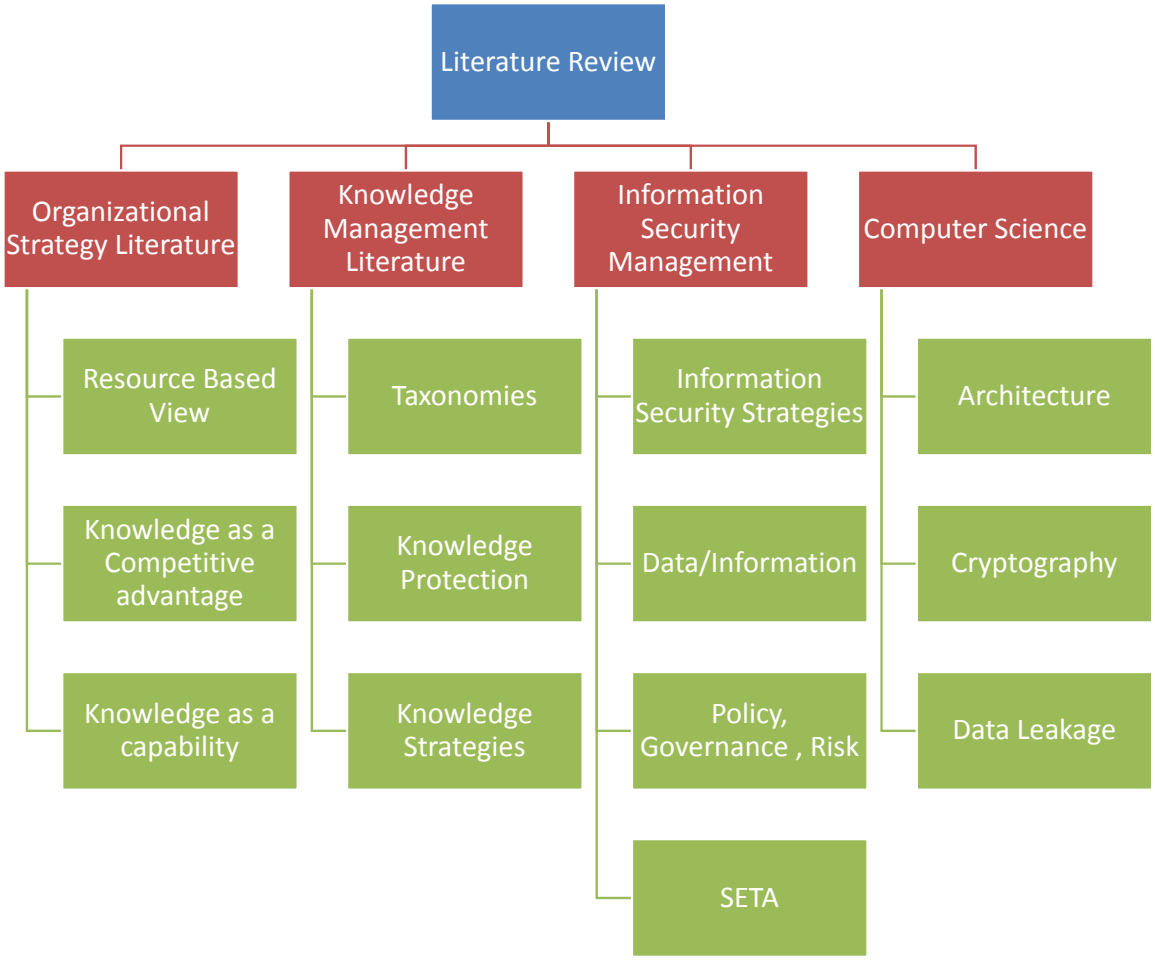
Key Question

- How Can Organizations protect their Information and Knowledge Assets?
  - What Security strategies can be used to protect Information and Knowledge assets?
  - How can these security strategies be deployed to protect Information and Knowledge assets?

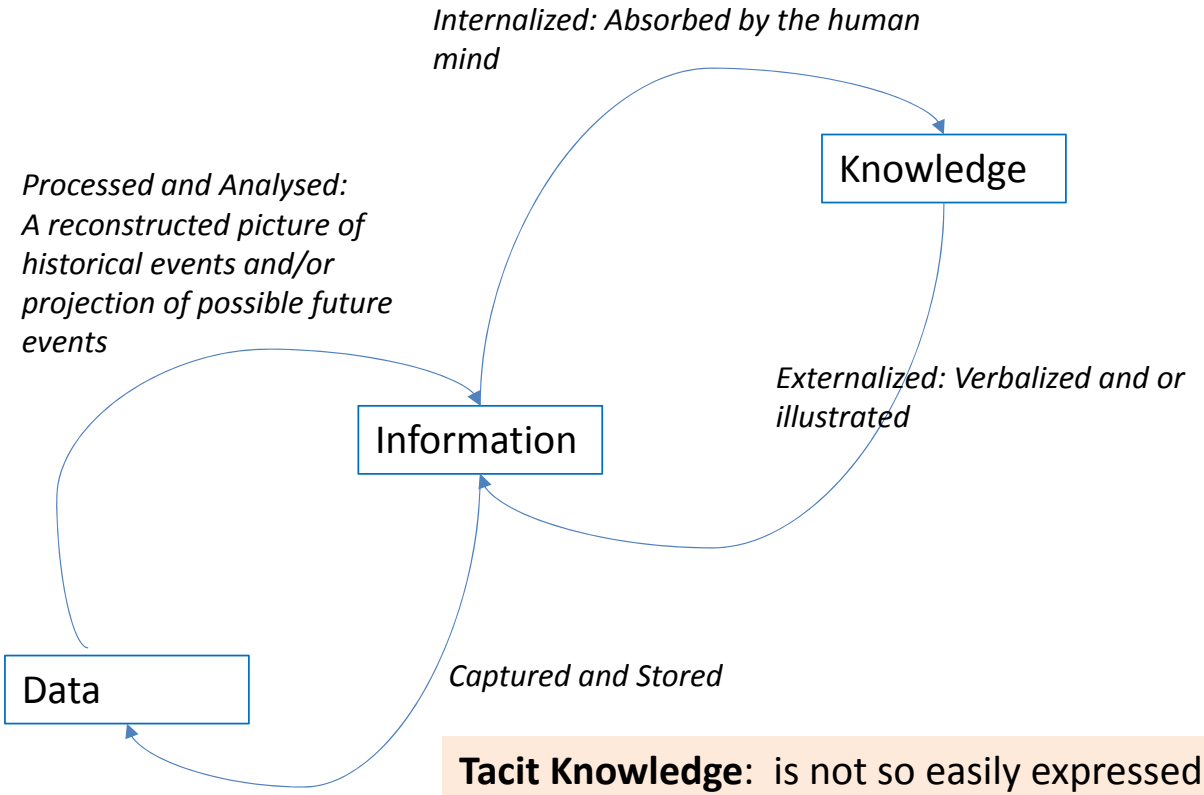
Although leakage can happen through technology, it frequently happens through other means (e.g. people, paper, conversations) making the problem of security broader than IT.

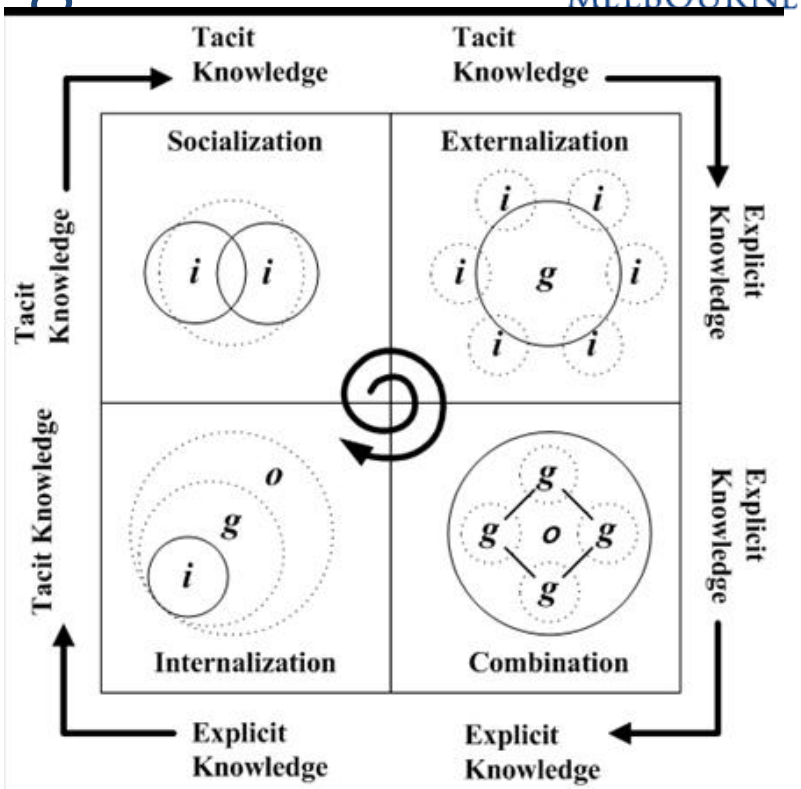
Most organizations have IT security capability but not leakage mitigation capability.

Relevant Literature



Data vs Information vs Knowledge

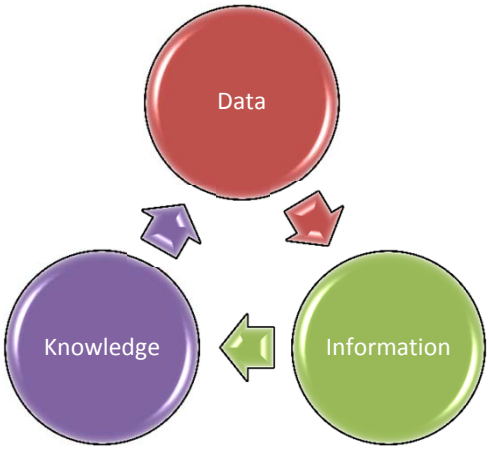




Tacit Knowledge: is not so easily expressed. It is highly personal, hard to formalize and difficult to communicate to others. It may also be impossible to capture.

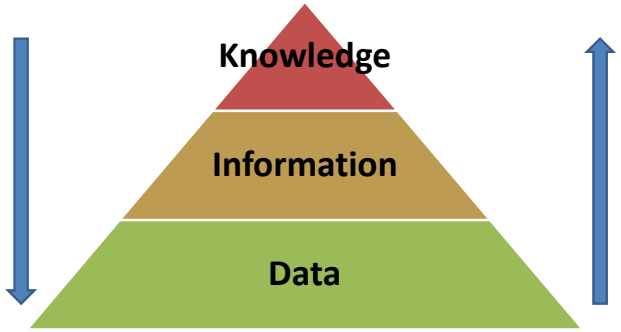
Explicit Knowledge: is formal and systematic. It can be easily communicated and shared. Typically, it has been documented.

Knowledge Cycle



Once knowledge has been made explicit (codified) into artefacts (text, video, audio, picture) then It becomes information (data) **(Alavi and Leidner, 2001).**

Thus, in this research we argue that it is possible to infer knowledge from information (a knowledge object) which can enable an unauthorized party to cause harm in the form of, for instance, competitive advantage erosion, loss of reputation or financial/legal liabilities. ***(Alavi and Leidner, 2001;)***



Knowledge

- Knowledge is defined as:

  A fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information. It originates and is applied in the minds of knowers. In organizations, it often becomes embedded not only in documents or repositories but also in organizational routines, processes, practices, and norms."

Davenport and Prusak (1998)

Perspectives on Knowledge from the KM literature

THE UNIVERSITY OF MELBOURNE

Perspective on Knowledge	Description
Knowledge vis-à-vis data and information. *(Fahey and Prusak, 1998)*	• Data is raw facts, raw numbers • Information is processed/interpreted data • Knowledge is personalized information, Value-added information
State of mind *(Schubert et al, 1998)*	Knowledge is the state of knowing and understanding
Object *(Carlson et al, 1996;Mcqueen,1998;Zack,1998)*	Knowledge is an object to be stored and manipulated (Knowledge stocks). Role of IT is to provide access to sources of knowledge rather than knowledge itself
Process *(Mcqueen,1998;Zack,1998)*	Knowledge is a process of applying expertise (Knowledge flows, creations, sharing and distribution), process of knowing and acting
Access to Information *(Mcqueen, 1998)*	Knowledge is a condition of access to information and should be organized to facilitate access to and retrieval of content.
Capability *(Carlson et al, 1996;Watson,1999)*	Knowledge is the potential to influence action, it is about building core competencies and understanding strategic know-how necessary in decision making.

Knowledge Leakage (KL)

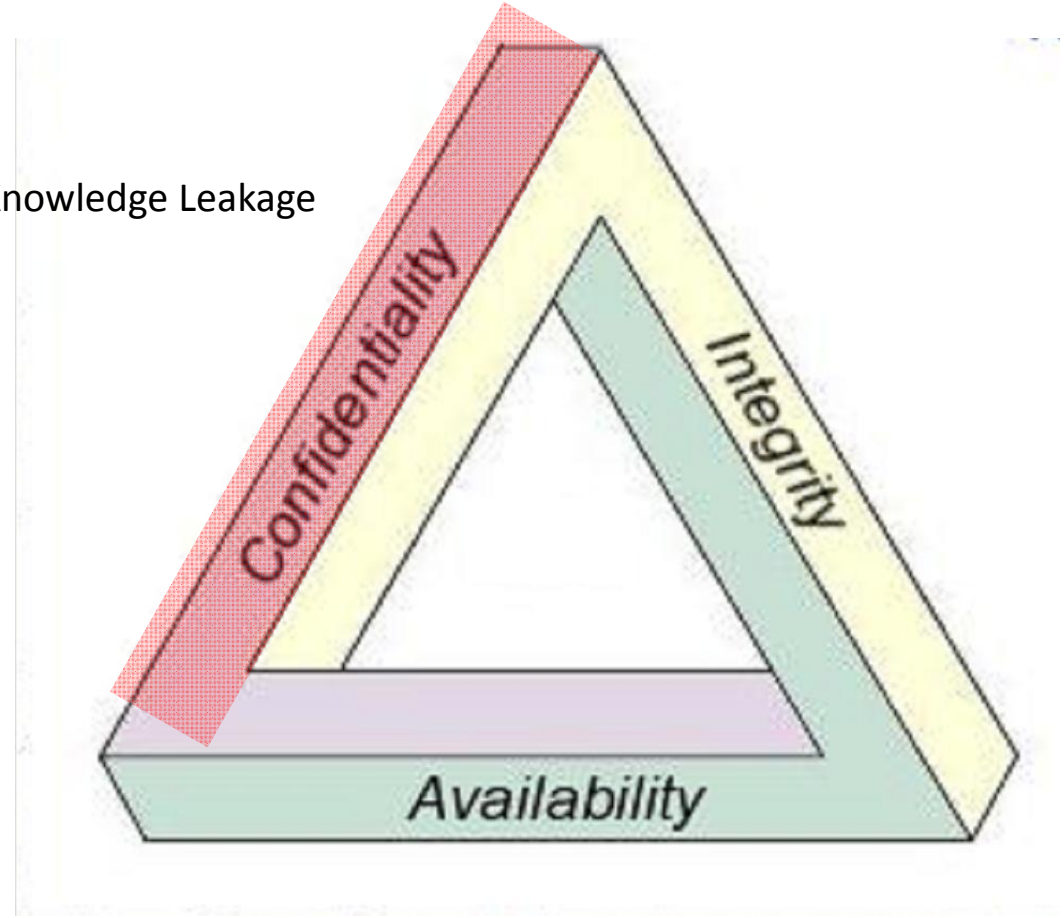
- ***Knowledge Leakage is defined by as:***

  "The accidental or deliberate loss or unauthorized transfer of knowledge intended to stay within an organization's boundary that may weaken the competitiveness and industrial's position of the organization".

(Annasigngh2006;Frishammar et. al. 2010)

Knowledge Leakage - Confidentiality

Knowledge Leakage



Knowledge Leakage

- **Intentional**
  - Disclosure of Knowledge
  - Copy of org. sensitive content
- **Unintentional**
  - Accidental email to recipient
  - Loss of staff (Experts leaving the organization)
  - Outsourcing/joint ventures
  - Employee oversight (Human errors/insider threat)
  - Poor business process
  - *Risky Behaviours*:
    - Posting confidential details on social media
    - click on phishing emails URLs unwittingly and download attachments from unknown sources
    - Connecting to open public Wi-Fi networks
    - Selection of poor security controls/ bypassing of controls (weak password)

Examples of Organizational Knowledge
Intellectual property
Trade secrets
Business Strategies
Product designs

Verizon Report, 2015

Example Scenarios

Different focus, Different Approach

- Data Leakage
  - Bits and bytes
  - Files, Stream of bytes
  - **Measures**: Data prevention Loss, encryption, firewall, antivirus, etc
  - Confidentiality, Integrity, Availability

Technical Approach

- Information Leakage
  - Databases, Emails,
  - **Measures**: Data prevention Loss, encryption, firewall, antivirus, etc
  - Confidentiality, Integrity, Availability

Technical Approach

- Knowledge Leakage
  - Knowledgeable employee leaves company to competitor
  - Knowledgeable Conference, meetings, chats
  - Inference knowledge from real-world interactions as opposed to digital-interactions (Metro, airport, restaurant , café) e.g., Shoulder-surfing,
  - **Measures**: Knowledge Protection, Legal (NDA, Patents, contracts) Copyright, Tacit Knowledge, Compartmentalization, disruption, misinformation, Knowledge Protection Policies,
  - Confidentiality, Knowledge Protection, Knowledge Retention, Security Risk exposure (perceived)

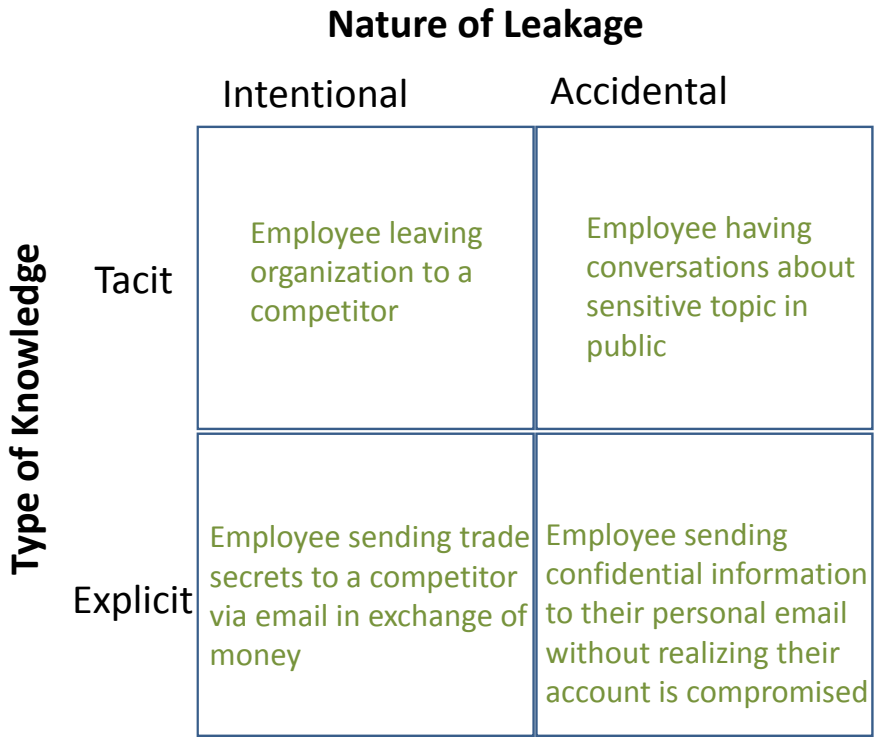
Human Approach

Knowledge Leakage Risk (KLR) - Definition

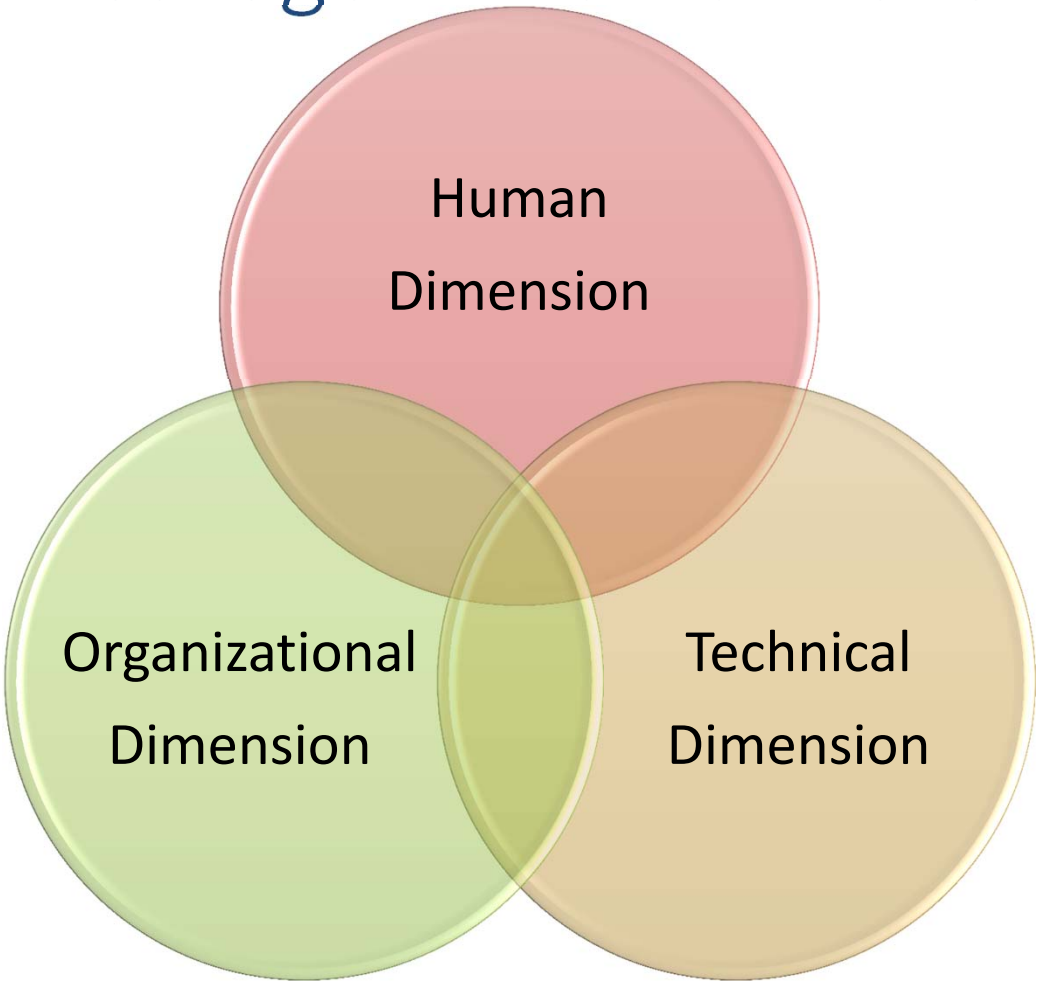
- A **measure** of the extent to which an organization is **threatened** by a potential Knowledge Leakage (KL) **circumstance** or **event**, and typically a function of :
  - (1) the **adverse impacts** that would arise if the KL circumstance or event occurs and
  - (2) the **likelihood** of the occurrence

KLR = KL Impact x KL Likelihood

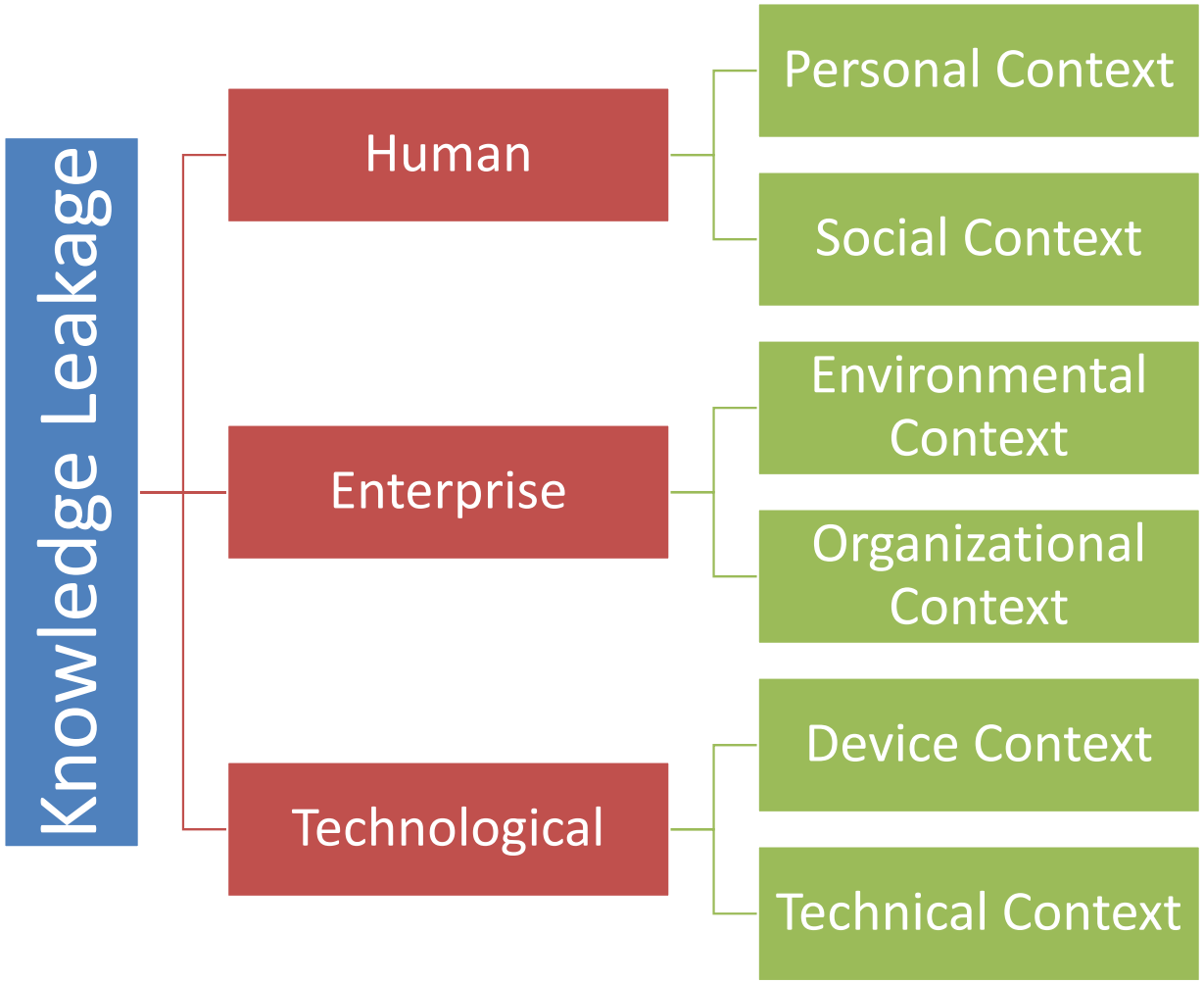
Knowledge Leakage Framework



Knowledge Leakage – Multidimensional Prob



Knowledge Leakage Contexts

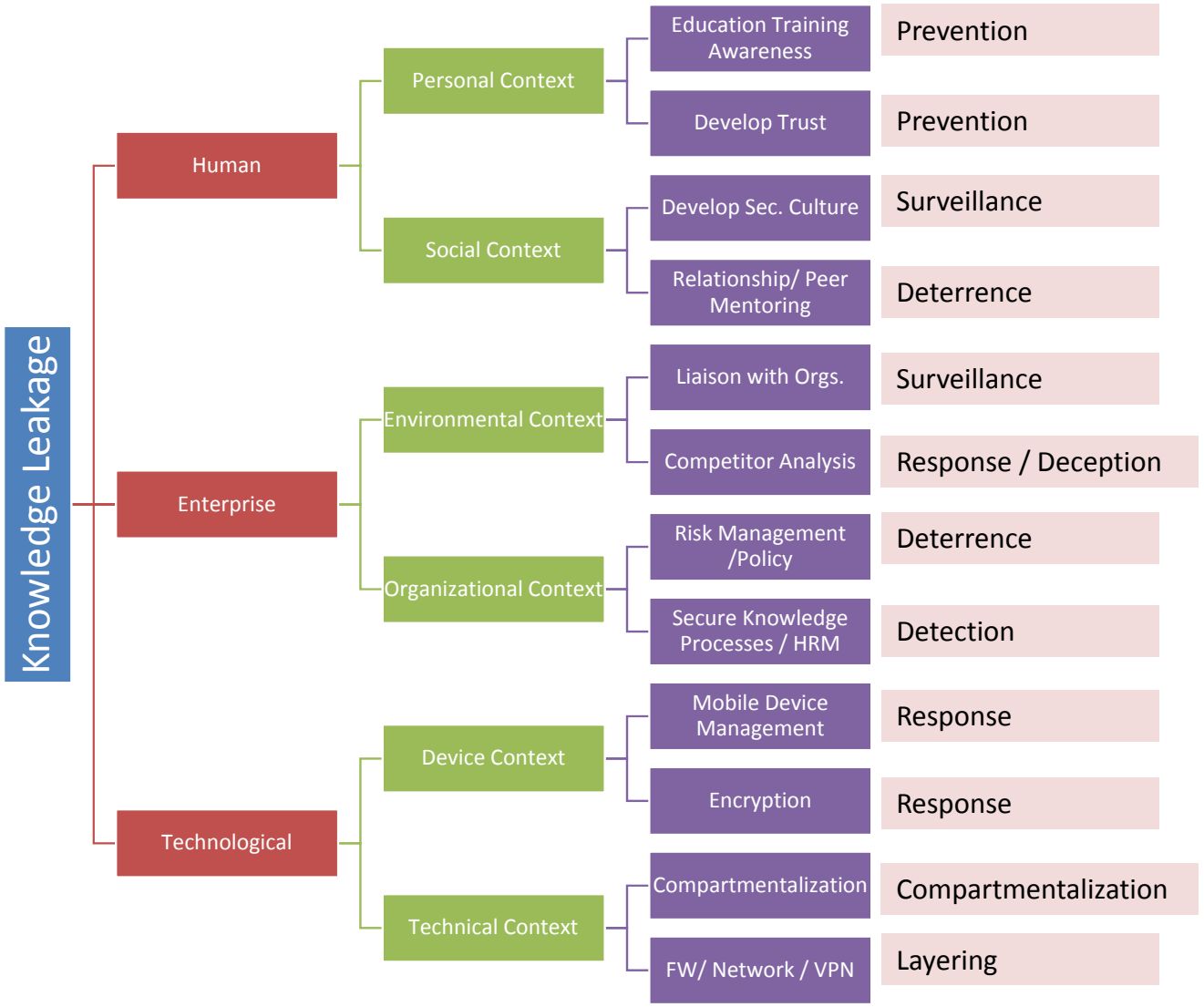


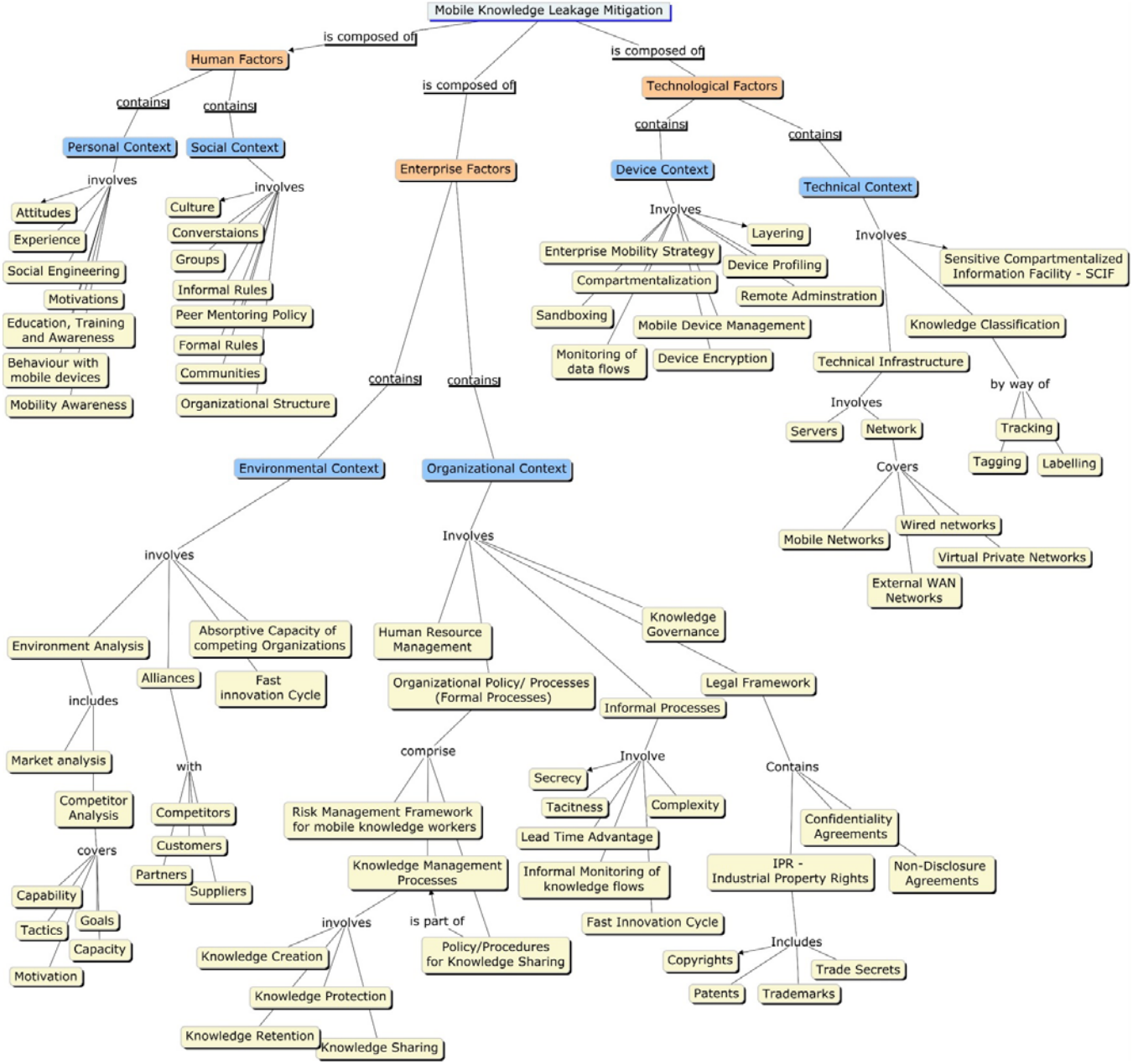
Security Strategies that can be used to combat Knowledge Leakage

THE UNIVERSITY OF MELBOURNE

1. **Prevention** : Protects assets by prohibiting unauthorised access , modification , destruction or disclosure
2. **Deterrence:** Employs disciplinary action to influence behaviour and attitude
3. **Surveillance:** Systematic monitoring to develop situational awareness
4. **Detection:** Identification of specific security behaviour
5. **Response:** Takes appropriate corrective actions against identified attacks
6. **Deception:** Distracts an attacker's attention from critical assets using decoys to waste their resources
7. **Perimeter Defence:** Creates a boundary around critical assets
8. **Compartmentalization:** Divides the intended area of attack into zones that are secured separately
9. **Layering:** Uses multiple countermeasures that function independently increasing the effectiveness of the defence.

Taxonomy K.L Strategies




Mobile Knowledge Leakage Mitigation
is composed of
Human Factors
is composed of
Enterprise Factors
is composed of
Technological Factors
contains
contains
Personal Context
Social Context
contains
contains
Device Context
Technical Context
involves
involves
Involves
Involves
Attitudes
Experience
Social Engineering
Motivations
Education, Training and Awareness
Behaviour with mobile devices
Mobility Awareness
Culture
Converstaions
Groups
Informal Rules
Peer Mentoring Policy
Formal Rules
Communities
Organizational Structure
Layering
Enterprise Mobility Strategy
Device Profiling
Compartmentalization
Remote Adminstration
Sandboxing
Mobile Device Management
Monitoring of data flows
Device Encryption
Sensitive Compartmentalized Information Facility - SCIF
Knowledge Classification
Technical Infrastructure
by way of
Involves
Servers
Network
Tracking
Tagging
Labelling
Covers
Mobile Networks
Wired networks
Virtual Private Networks
External WAN Networks
contains
contains
Environmental Context
Organizational Context
involves
Involves
Environment Analysis
Alliances
Absorptive Capacity of competing Organizations
Fast innovation Cycle
includes
Market analysis
Competitor Analysis
covers
Capability
Tactics
Goals
Capacity
Motivation
with
Competitors
Customers
Partners
Suppliers
Human Resource Management
Organizational Policy/ Processes (Formal Processes)
Knowledge Governance
Informal Processes
Legal Framework
comprise
Involve
Contains
Risk Management Framework for mobile knowledge workers
Knowledge Management Processes
involves
is part of
Knowledge Creation
Knowledge Protection
Knowledge Retention
Knowledge Sharing
Policy/Procedures for Knowledge Sharing
Secrecy
Tacitness
Complexity
Lead Time Advantage
Informal Monitoring of knowledge flows
Fast Innovation Cycle
Confidentiality Agreements
IPR - Industrial Property Rights
Non-Disclosure Agreements
Includes
Copyrights
Trade Secrets
Patents
Trademarks

Methodology

- **Qualitative** Research Design (Due to the explorative nature of this study)
- Data Collection:
  - 20 x **Interviews** (1 h. approx.) conducted in **Australian** knowledge-intensive organizations to:
    - Security Managers
    - Knowledge Managers
  - **Supplementary** Information analysed for **triangulation**
    - Standard
    - Policies
    - Procedures
    - Guidelines
  - Design of KL **Scenarios** caused by Mobile Devices to discuss with Managers and their **strategies** based on the **Research Model**

THE UNIVERSITY OF MELBOURNE

Preliminary Findings

Human Factor – Personal Context

- Develop Trust –
- Use of Deterrents (formal punisments, sanctions)
- High Risk person / High Risk position - People of Concern
- -User Behaviour Analytics (Artificial Intelligence - profiling)
- -Gamification (Simulation of scenarios) to influence behaviour
- - Education, Training and Awareness for knowledge sharing through mobile devices
- Decoy campaigns deployed to their mobile device

> *"our CEO always says: if people are the weakest link then education is the strongest link, this is why we are investing in a comprehensive education program for our staff"* [SM2]

Human Factor – Social Context

- -Develop a Mobile Security Culture – Security habits
- Use of Deterrants (punisments, sanctions)
- -Knowledge Communities / Portal (Tips, reminders, HR mood boost)
- -Peer Mentoring Policy (Encourage them to Always ask questions)

> *"The good thing about the program that we started a few years ago is that now the employees teach the new staff our values and principles and often I see how they report any suspicious activity before actioning on requests coming from strangers or emails"* [KM4]

Enterprise Factor – Organizational Context

- **Mobile Risk Management** Framework (Identification of valuable knowledge assets) – Who knows what -
- Standard, Policy & Procedures for mobile workers.
- Legal Framework (IP Protection Mechanisms: Patent, trade secrets, copyrights, trademarks,NDA)
- Embed security into Knowledge processes to protect when using mobile devices.
- Human Resource Management to deal with Tacit Knowledge – knowledge Governance

- Knowledge Protection Roles
- Protection of Knowledge flows
- Embed Extra complexity into processes
- Constant Monitoring to mobile workers dealing with sensitive knowledge
- -Knowledge Management Strategy
- -Develop resilience capability
- -Knowledge reconfiguration (combine knowledge assets to create new knowledge)
- -Multi-disciplinary integration among org. areas (e.g., HR, IT, Legal, Finance)

"We have a really strict screening policy, once a knowledgeable person leaves the organization, in fact, the policy states that screening is on-going. So when you join the company you have to undertake a long screening process and after that every year HR reminds us the process and even when you leave you need to follow an exit policy to make sure there is no liability for the company" [KM1]

Enterprise Factor – Environmental Context

THE UNIVERSITY OF MELBOURNE

- -**Liaisons** between organizations (Government, Research, private and public sector)
- Factors to deter knowledge (**Tacitness**, deliberate **barriers** to limit **K. Transfer**)
- -Market analysis (Fast Innovation Cycle)
- -Competitor/Adversary Analysis (Tactics, Motivation, Goals)
- Counter-intelligence techniques on Mobile settings
- Working off-site Policies (Mobile workers & Tele-workers)
- Conversation & behaviours outside organizational boundaries (Mobile workers & Tele-workers)

"So far we have different partnerships with universities in the UK and the US to help us with research and development of technologies, however we only give them the bare minimum just to make sure there's no chance of a breach and they usually work in another location isolated from us" [CISO2]

Technological Factor – Device Context

- Mobile Device Management (MDM)
- -Mobile Device Usage Policy
- Encryption (codified knowledge-information)
- -Geolocation settings (Environment-aware)
- -Device Sandboxing (Compartmentalization)
- -Remote administration – Unsecure WI-FI detection and blocking
- -Device Profiling (Usage Pattern-Analytics)

"We use a feature within Airwatch that is called Secure Content Management that allows our mobile force to access documents on the go through their laptops, iPads or iPhones but the physical location of the document is on our servers so if anything happens we just revoke access to the content without messing with their equipment" [SM3]

Technological Factor – Tech. Context

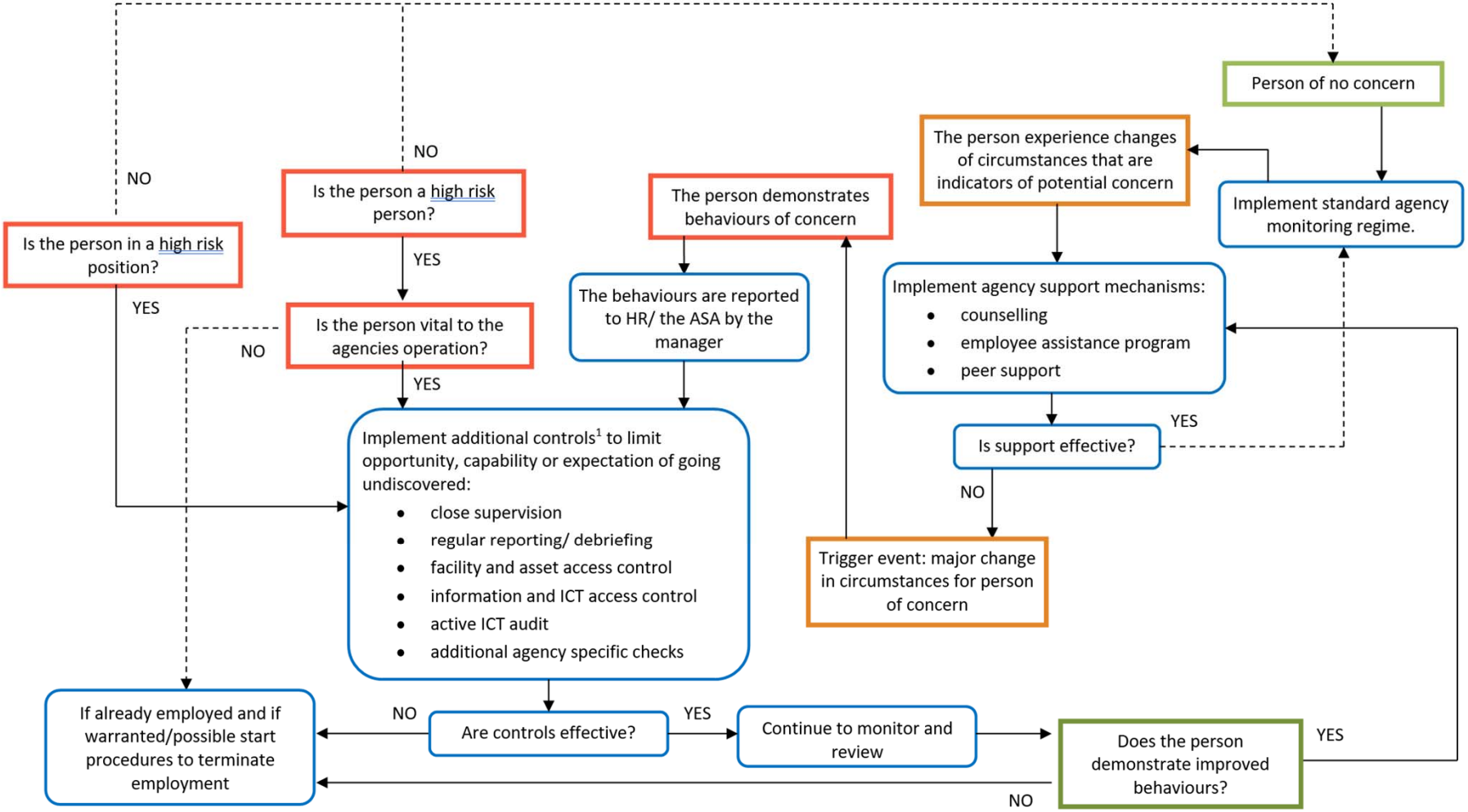
- -Enterprise Mobility Strategy
- - Mobile Device Usage Analytics (Artificial Intelligence)
- -Knowledge Compartmentalization (access, clearance)
- -Knowledge Classification (tagging, labelling)
- Authentication, Control and Tracking of documents

"What I love about our SIEM is that it displays a nice dashboard showing the patterns for a particular individual, so we know more about their usage and their profiles and sometimes it even notifies us when a possible person may be at risk of leaving the organization as their behaviour changes and, for instance, starts sending a lot of company information to other accounts outside our authorized domains." [CIKO]

THE UNIVERSITY OF MELBOURNE

Supplementary Documentation

Annex 1: Decision map - Managing people of security concern



1. Only action in a way that does not compromising any ongoing investigations

Organisational personnel security	Make sure you: • know your business • have a good security culture • perform a personnel security risk assessment • understand the legal framework • communicate personnel security and the consequences of personnel security breaches to your employees.
Pre-employment personnel security	Perform the following pre-employment background checks: • identity checks, including overseas applicants or applicants who have spent time overseas • qualification and employment checks • national criminal history checks • financial background checks. All documents for the checks should be secured. Any applicant who fails to meet the standard of your business should be rejected for employment.
Ongoing personnel security	Make sure you: • have access controls in place • perform protective monitoring • promote a security culture, including – counter manipulation – report and investigate, when necessary – perform ongoing checks – submit contractors to the same security clearance as in-house personnel • recognise after employment threats.
Information and communications technology security	Be sure to consider and, if necessary, monitor: • electronic access • shared administrative accounts • account management policies and procedures • the standard operating environment • system logs.

Table 1 – A personnel security framework

Annex A—Checklist for mobile computing and communications/tele-working

- ☐ Has the employee been required to read, or been briefed on the requirements for the protection of official resources?
- ☐ What is the security classification or sensitivity of the official resources to be removed?
- ☐ Why are the official resources being removed off-site?
- ☐ How long will the official resources be off-site?
- ☐ Have the details of the official resources being removed been recorded?
- ☐ Do the official resources being removed belong to another agency? If so, has that agency given its approval?
- ☐ How will the official resources be securely transferred or transported?
- ☐ Is the removal of the official resources from the agency a temporary/one off or a permanent/long term arrangement?
- ☐ How will the official resources be securely stored off-site?
- ☐ What is known about the location where the resources are being taken? Is a risk assessment needed in relation to that location?
- ☐ What control does the agency have over the security of the location?
- ☐ Who has access to the location where the official resources are being stored?
- ☐ How will the employee protect his/her work from unwanted scrutiny or unauthorised access?
- ☐ How will the employee protect his/her official conversations from being overheard?
- ☐ Could the resources being carried reasonably expose the employee to targeting by a foreign intelligence service? Has the employee been appropriately briefed? See Contact Reporting Guidelines.
- ☐ Is the employee aware of what action he or she is to take in the event official resources are stolen?
- ☐ Is the employee considering printing, duplication or disposal of official information in a non-secure environment? What measures have been put in place to ensure official information is not compromised by this activity?
- ☐ Has the agency authorised the use of any off-site ICT equipment? If so what equipment and in what circumstances?
- ☐ Does the employee have an authorised email account, or remote ICT access to agency systems, that can be accessed securely?

Discussion

THE UNIVERSITY OF MELBOURNE

- Organizations are **well aware of the risk of KL** caused by the use of Mobile devices and the consequences to their competitive advantage
- Some organizations still confuse operational information with organizational knowledge. At the Technological context, knowledge is treated as information and protected as such (Encryption).
- The focus is slowly shifting away from Tech. and towards Process and People and **HR** as a way to deal with KLR (**HRM**)
- It is not about **mobile** as much as it is about *understanding* **mobility**
- There is a confusion between tele-workers and mobile workers
- Organizations are starting to create Knowledge Protection Processes in mobile workflows
- In order to protect knowledge in mobile contexts, a lot of organizations develop **informal protection mechanisms** (complexity, lead time advantage, innovation cycle timing, secrecy, misinformation)

Discussion – cont.

- Dialectical opposition between KM and SM
- Knowledge protection mechanisms for Tacit knowledge vs. Explicit Knowledge (Knowledge already articulated, codified)
- Although it is argued that Tacit knowledge cannot leak, Tacit knowledge on its way to being articulated can definitely leak (e.g., conversation).

Contributions

Our study makes the following contributions:

- Developing of a **conceptual model** grounded on the mobile context and Knowledge leakage literature that was used to categorize the evidence found in interviews. This **categorization** can be valuable for future research and organizations seeking to understand and assess their KLR mitigation strategies.
- Synthesis of different Knowledge-leakage related mechanisms reported by organizations in our study and categorized into Human, Enterprise and Technological dimensions.
- The study also highlight the following empirical observations:
  - Organizations are aware of the KLR caused by Mobile Devices
  - Dichotomy between Mobile and Mobility (behaviour)
  - The call for design knowledge protection processes into mobile workflows
  - The use of **informal** protection mechanisms to **prevent** knowledge leakage

Limitations & Future Work

THE UNIVERSITY OF MELBOURNE

- Limitations:
  - **Sample** was **specific** and **small** (Australian Organizations in some industries)
  - Main source of information was **interviews** with senior managers, as such we did not explore leakage-related behaviours at the **operational** level (**workers**)
  - Given the sensitive nature of knowledge leakage, incident information is difficult to obtain, as such we use scenarios as a proxy to gather information.
- Future Work
  - **Design**/**refinement** of a **maturity framework** based on the findings and the **levels of strategy sophistication** followed by organizations with **different KLR exposure.**
  - Conduct of **focus groups** (KM & SM) to **validate** and **evaluate** the Maturity Model and our findings.