

INSETA Research Chair: Digitalisation

PROF COLIN THAKUR

30 JULY 2021

PRESENTATION ON RESEARCH PROGRESS

Measuring Occupational Change: Firm-level Studies

Research Proposal

PROF HOOSEN RASOOL

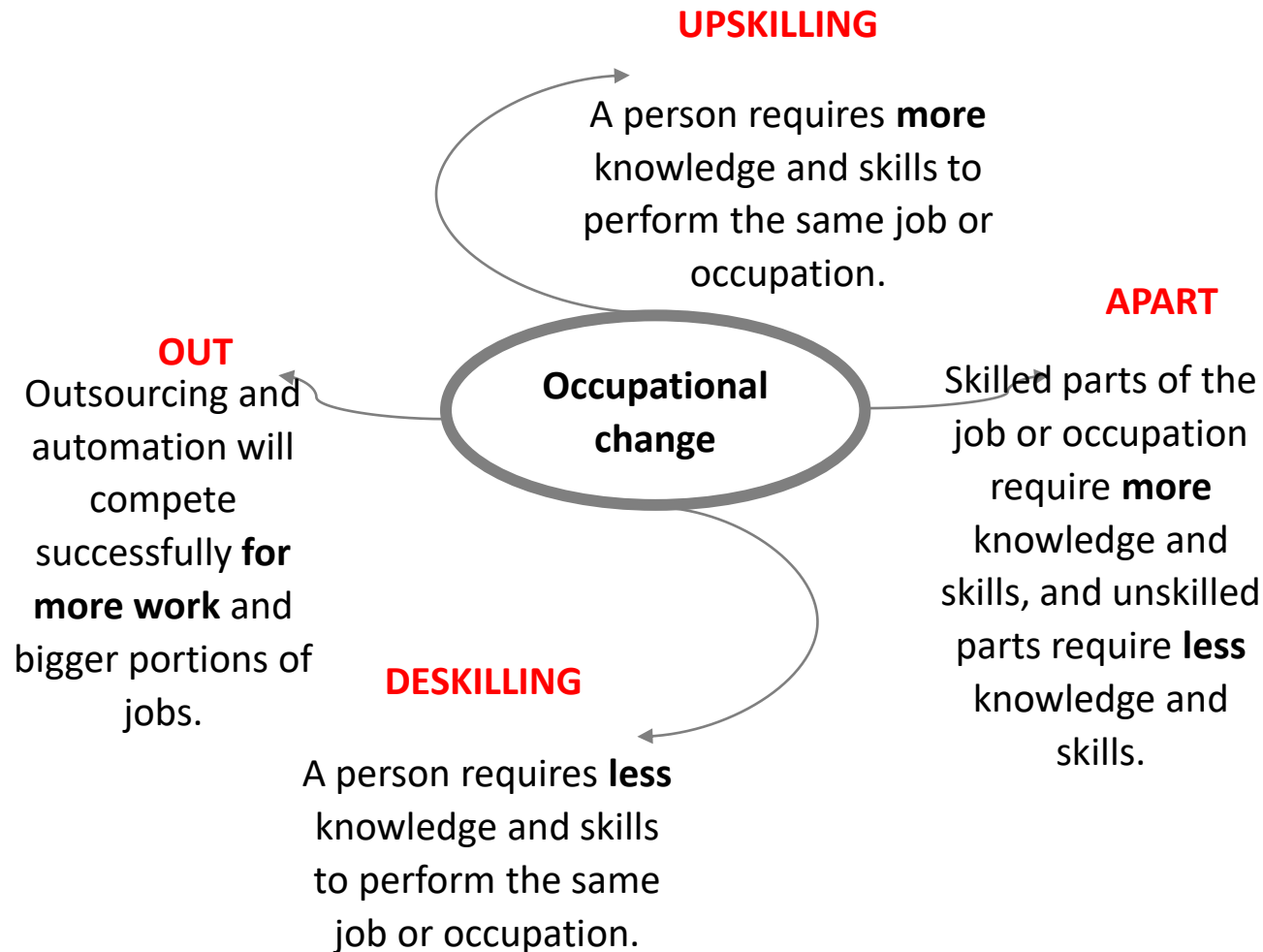
Background to the Research

In 2020, the DUT Research Chair conducted a research study :

“Measuring occupational change in the insurance sector: approaches, methods and processes”.

There is now a need to measure occupational change in key occupations in insurance firms as a second phase of the research.

Assumptions

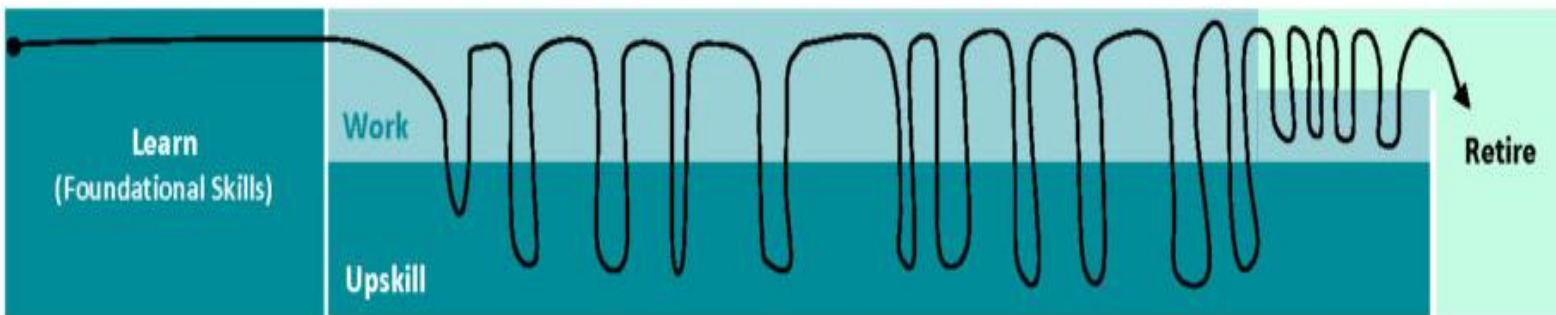


Trends

Traditional Model:



Lifelong Learning Model:



Trends

FUTURE OF WORK: WE MUST RETIRE THESE QUESTIONS

We ask young people: “WHAT do you want to be when you grow up?”

65%

of jobs do not yet exist

We ask university students: “WHAT is your major?”

47
%

of tasks will be automated by 2033

We ask each other: “So, WHAT do you do [for a living]?”

17 / 5

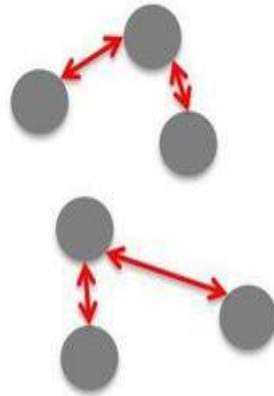
The person will work in
about 17 jobs in five industries

Trends

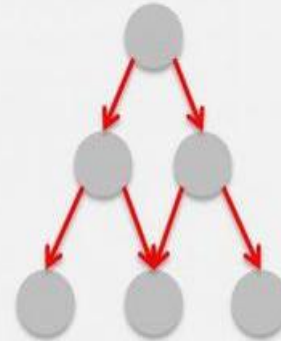
The Evolution of Work, Jobs and Occupations



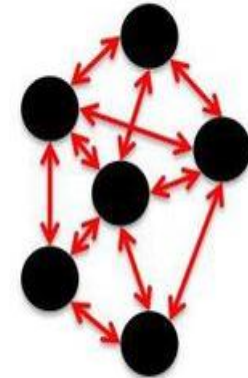
Do
Everything
Yourself



Learn A
Barter-able
Skill



Hyper-Focus
On A
Marketable
Skill



Learn To
Learn, Adapt
+ Create New
Value

TOP 10 SECTOR PRIORITY OCCUPATIONS IN INSETA SECTOR SKILLS PLAN

Insurance Agent	Actuary	Software Developer	Insurance Broker	Developer Programmer
Insurance Loss Adjuster	Claims Administrator	Financial Investment Advisor	Compliance Officer	Sales and Marketing Manager

Occupational Mapping II

Case Study

Three firms (small, medium and large) will be identified and key occupations will be measured.

An analysis of current and future skills needs of insurtechs

Research Proposal

PROF HOOSEN RASOOL

Background to the Study

- ❑ Financial technology (fintech), known as insurtechs in the industry, is transforming the financial services sector across the globe.
- ❑ SA has a small but fast-growing fintech industry, presenting considerable benefits and risks.
- ❑ Insurtechs are advanced technology insurance firms that have the potential to transform the provision of insurance services and products spurring the development of new business models, applications, and whose products and services are directly applicable in the delivery of financial services.

Background to the Study

An important development to consider is how the insurance sector responds to economic and societal technological innovations, and provides insurance processes and policies that incorporate such changes.

Problem Statement

- ❑ SA does not have a shortage of funding channels. However, many of the challenges are not accessible to insurtechs because they have yet to develop a proven business model, have not yet secured regulatory compliance and have yet to scale up.
- ❑ The low quality of inclusion products in SA creates opportunities for insurtechs to address consumer segments that are not currently served by traditional insurance service providers.

Outcomes/ Purpose of the Study

- ☐ Provide an analysis of the insurtechs landscape in SA.
- ☐ Identify the key occupations and skills sets required for insurtechs
- ☐ Determine new qualifications and skills programmes that should be developed by the QCTO.
- ☐ Identify current and future occupations and skills needs for insurtechs.
- ☐ Develop learning and career pathways for new entrants into the insurance sector.

Research Methodology

Literature review

A literature review of the following will be conducted:

- ✓ Insurtech types
- ✓ Role of insurtechs in addressing the lower end of the market
- ✓ Current and future skills sets

Case Study

Case study of two insurtechs

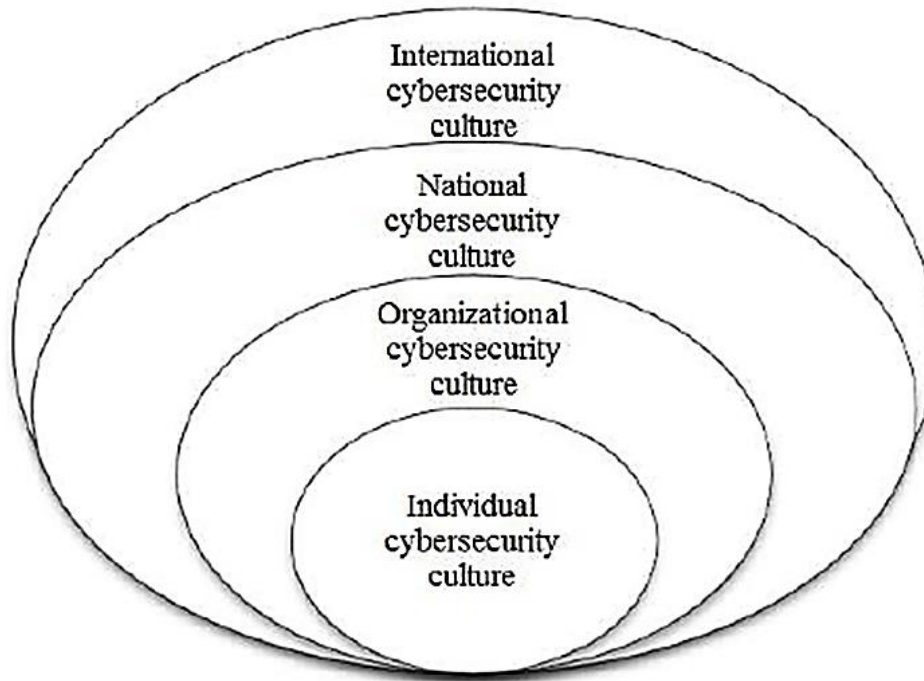
Cybersecurity Culture at TVET Colleges:

Literature Review

DR ZORAN MITROVIC

The idea

“To effectively deal with Cybersecurity, it is prudent [...] ensuring South Africa has a culture of Cybersecurity.”
(SA Government Gazette, 2015).



da Vega (2016)

- Due to the **lack of awareness and knowledge**, the idea was to **build cybersecurity culture** within **TVET colleges** that have a **potential to spread** through the **surrounding communities** where teachers and students live.

The task at hands

- It is **essential** to generate and maintain the **positive attitude** of TVET **teachers** and **students** towards digital technology and **readiness** and **ability** to **use** it securely (Lange, Hofmann & Di Cara, 2020; Bandara et al., 2014).
- The above **facts** have **motivated** the **need** for creating an **Action plan** for **building cybersecurity culture** in TVET colleges that **have** a **potential** of **influencing** cybersecurity culture in the surrounding **communities**.
- The reviewed literature suggests that **knowledge** and **skills** having **crucial role** in **preventing cyber-attacks**.
- Hence the need for **speeding** up cybersecurity **awareness** and **skill acquisition** by students and teachers in TVET colleges.
- **Youth** will only **be able** to **drive change** if they have the **sense** of the **power** to **make a difference** - this should be **prioritised** in **youth-centred development** strategies in general, (IFAD, 2019).

Literature review findings

- Schools are the **second uppermost target** for **ransomware** attacks.
- **Students** or **staff** that **circumvent** cybersecurity protections.
- HE cybersecurity **incidents** and **breaches** are caused by **social engineering** attacks (Impact, 2019).
- **Price of educational records** on the black market reaches **R 3,900** (USD 265) (ibid).
- **73%** of organizations are **unprepared** for cyberattacks and **many** of them **remaining** unprepared even **after** an **attack** (Inc, 2018).
- **85%** of **universities** agree that **more funding** must be given to **cybersecurity** (Purplesec, 2021).
- **Educational establishments** experienced the **sixth-most amount** of cybersecurity **incidents** out of **20 sectors**(Verizon , 2020).

Literature review findings (2)

➤ Dimensions of cybersecurity culture:

- Attitudes
- Behaviour
- Cognition
- Communication
- Compliance
- Norms
- Responsibilities

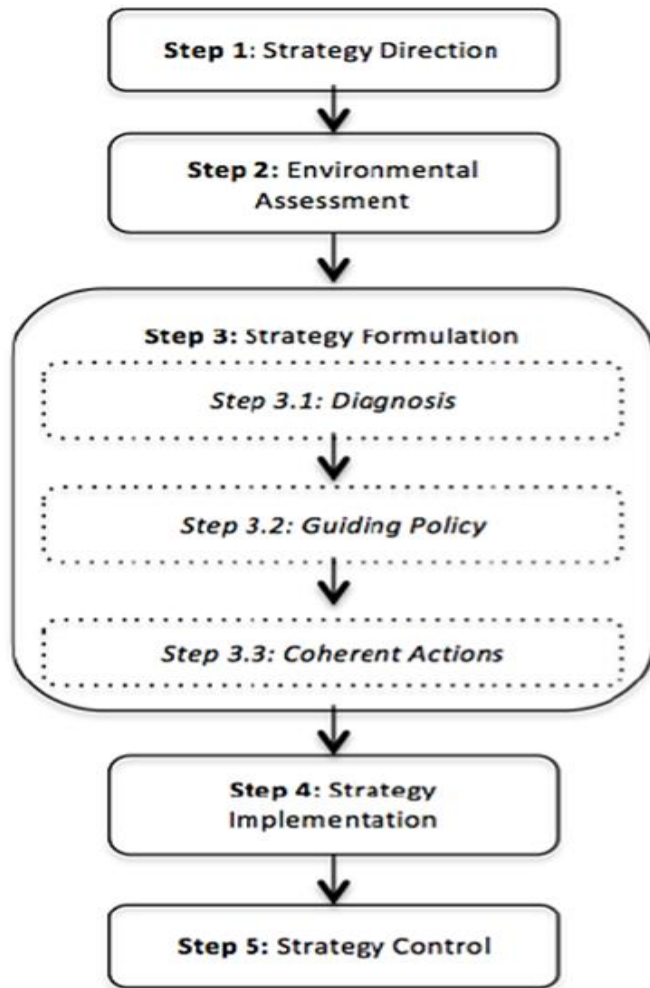
Factors impacting cybersecurity cultures:

- **Organisational** culture
- Wider **cybersecurity strategy**
- The **roles** to be played by **different groups** (e.g. CEO, CISOs, middle management, IT, HR, etc.)
- **Human factors** in cybersecurity culture (e.g. psychological factors, compliance and personality, the social environment)
- **External** factor: (e.g. National culture)
- Creating a **receptive environment**

Implementation of cybersecurity culture:

- **Frameworks** (e.g. ENISA Framework)
- **Syllabus** of the educational course on **cybersecurity culture: knowledge acquisition**
- **Activities** for delivering cybersecurity culture programmes (e.g. Online, hybrid, offline)

Literature review findings (3)



Measuring cybersecurity culture (e.g. ENISA, 2018) :

- **Approach 1: Determine a CSC current situation independently** from the CSC interventions
- **Approach 2: Determine a CSC current situation** by utilising the CSC intervention metrics
- **Approach 3: Combine approaches 1 and 2**

Towards constructing CSC conceptual model

- The literature review **main findings** are basically **elements** of the **conceptual** model of cybersecurity culture.
- The success of a CSC programme rests on a number of **key principles**(e.g. ENISA, 2018):
 - Secure **buy-in** at the **highest level**
 - **Follow** the **CSC Framework** for the **implementation** of the programme
 - **Know** the **organisation** so as to **ensure success**
 - **Measure** the **current cybersecurity** level of the **target audience**
 - **Draw** upon the **good practices** identified in this report.