Cybersecurity Leadership: Growing the Maconachy, Schou, Ragsdale (MSR) model to identify new cyber skills

Dr. Ervin Frenzel

10th annual CAE in Cybersecurity Community Symposium

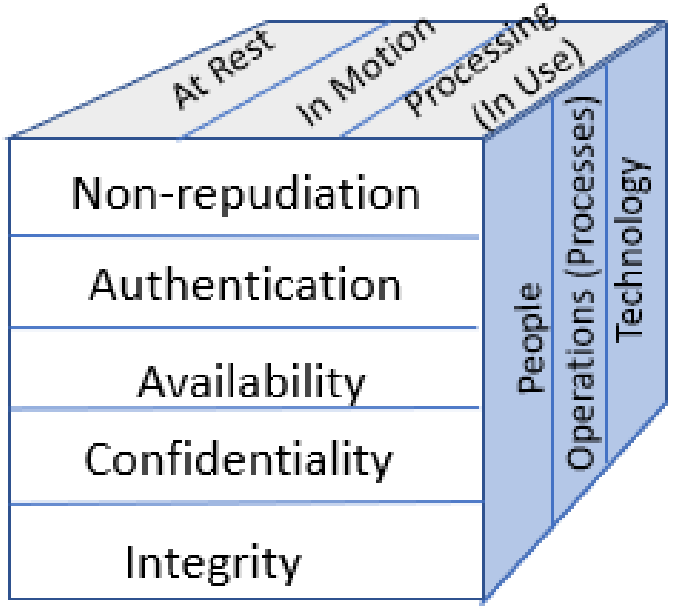
June 8-9, 2023

Seattle, WA

There is industry wide confusion over what is a cybersecurity technician?

Answering what is a cybersecurity technician provides a pathway to identification, classification, and eventual training of skills technicians need to fill identified shortages of both cybersecurity professionals and technical component level security.

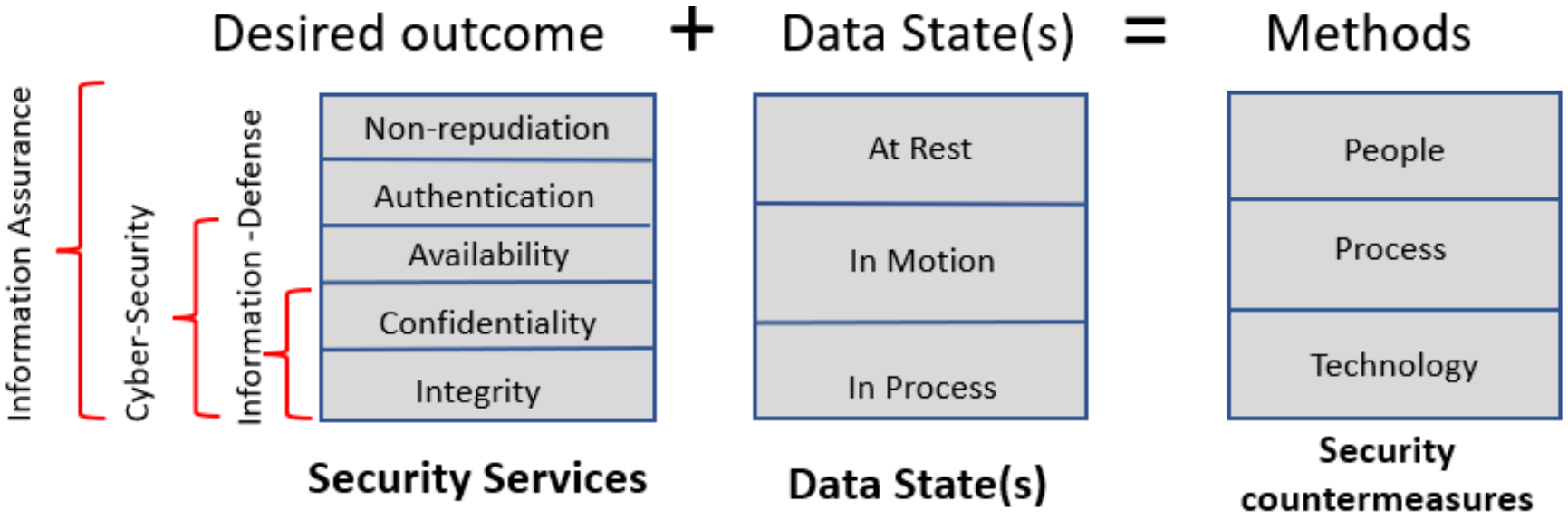
Traditional Viewpoint



As presented in normal (current) model:

Desired outcomes + data state = methods

Identifying the focus

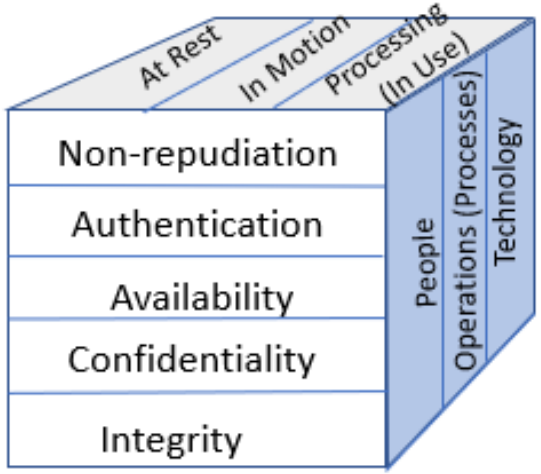


As presented in normal (current) model –

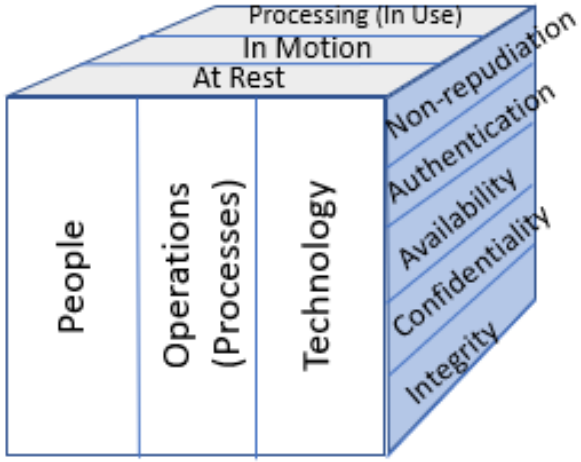
Desired outcomes + data state = methods

Changing the cube focus – changes our focus

Traditional Viewpoint

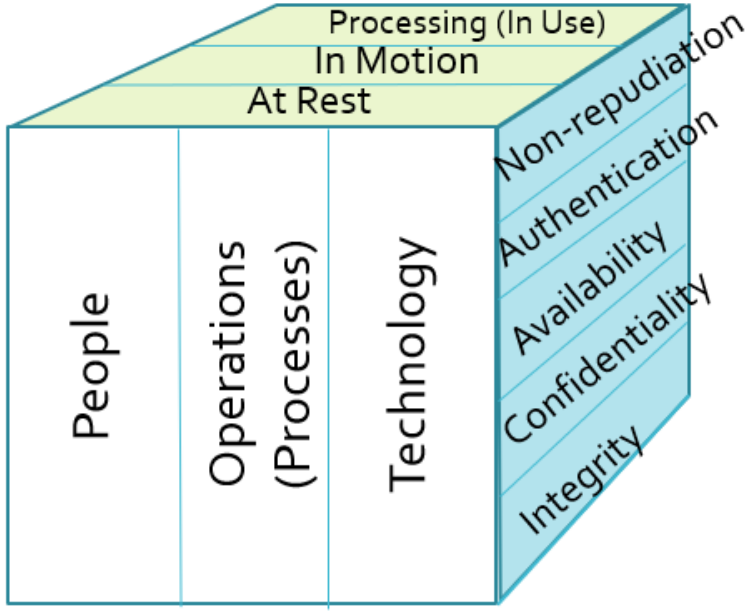


Recommended Viewpoint



Rotate the cube 90 degrees for best results

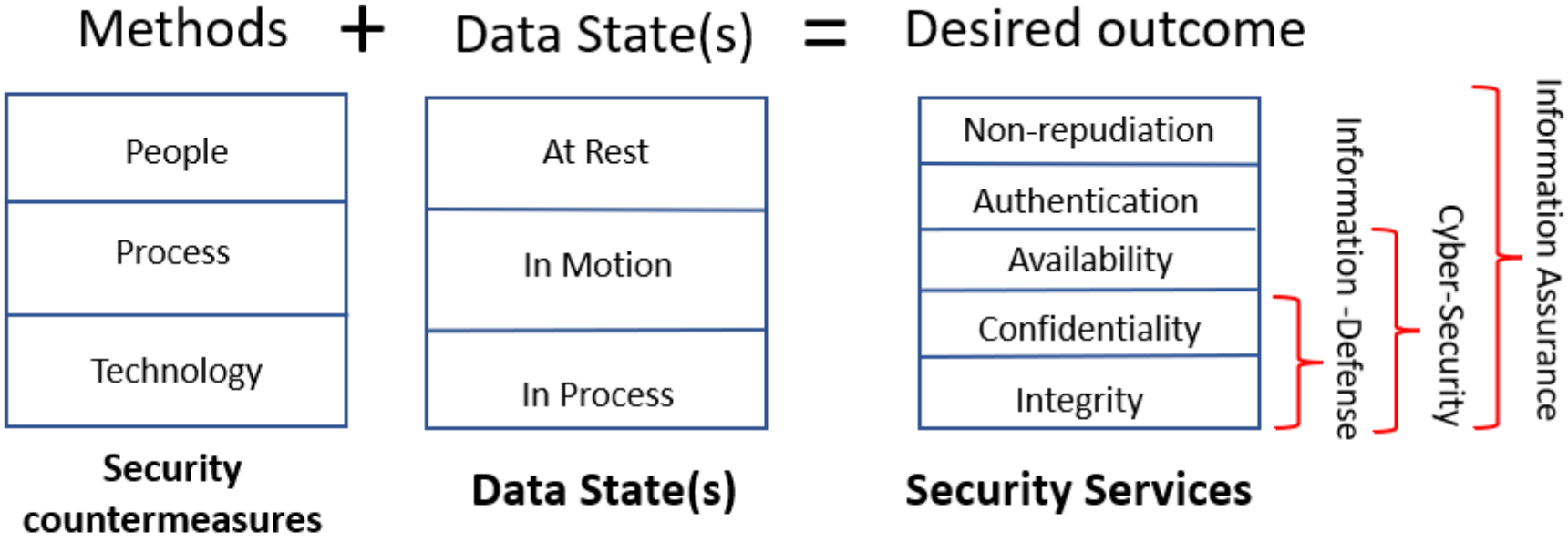
Recommended Viewpoint



As presented in proposed model:

Methods + Data State = Desired Outcomes

Shouldn’t our model be based upon using a method to get to a desired outcome instead?

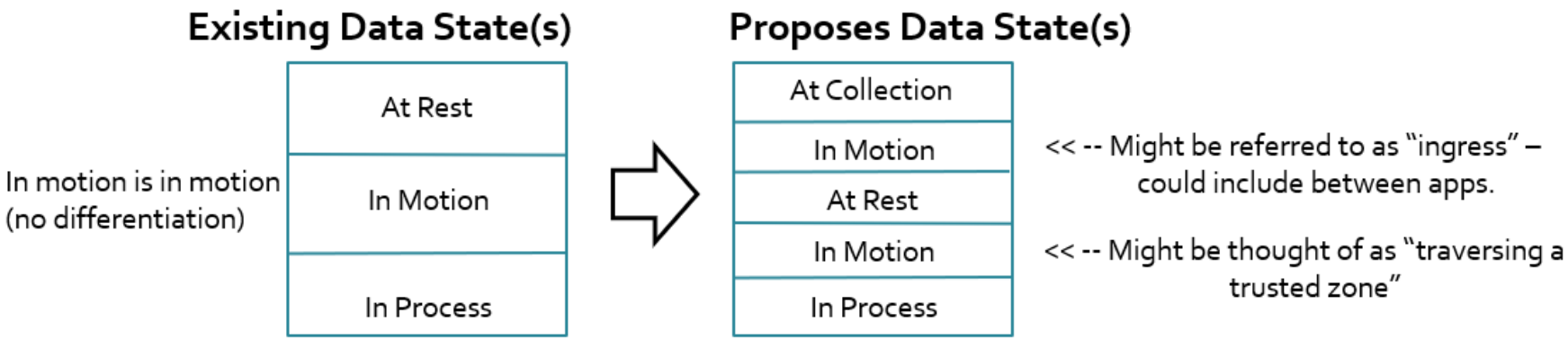


As presented in proposed model –

Methods + Data State = Desired Outcomes

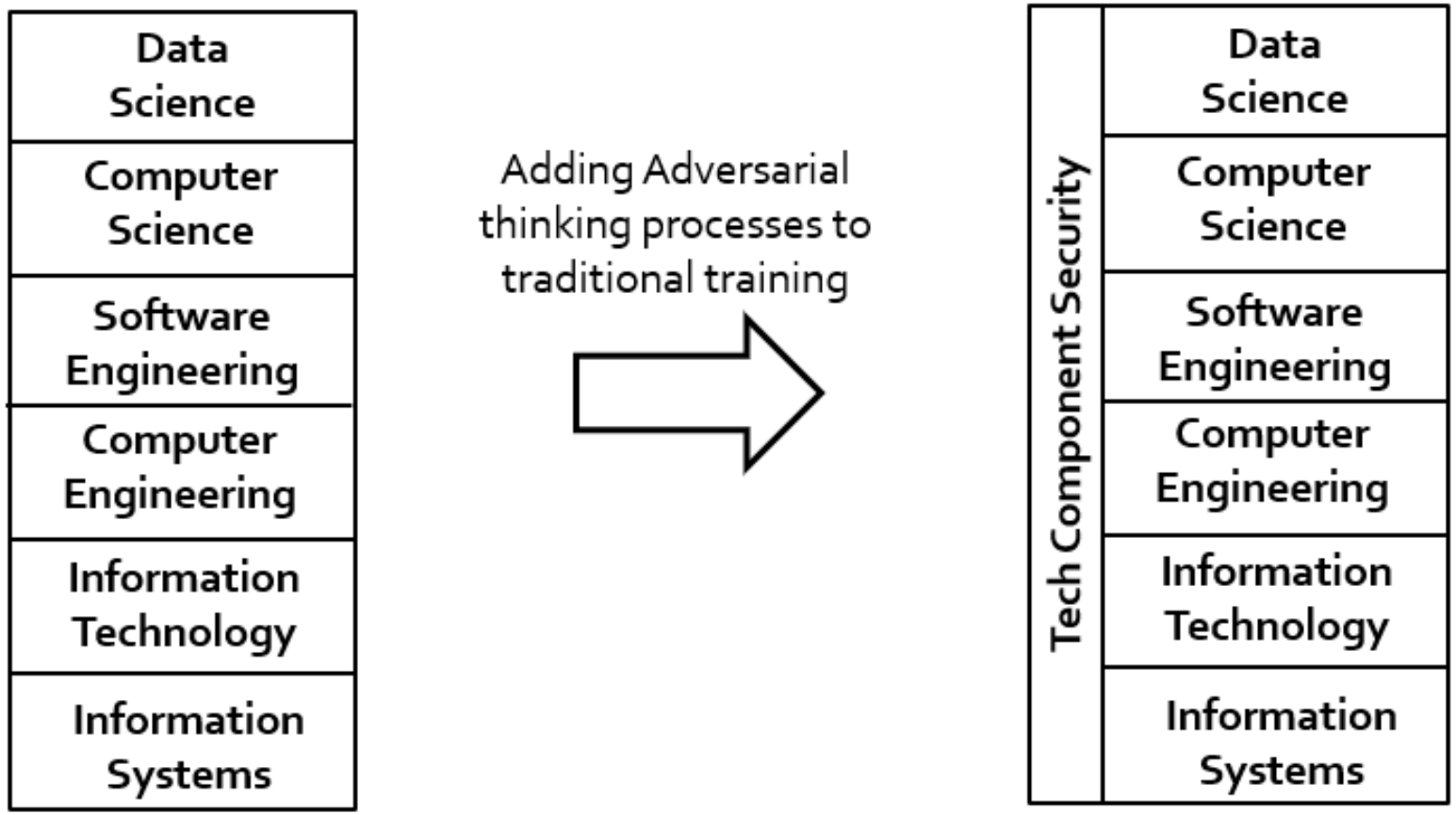
Our usage/ collection has evolved since 2001, organizations buy and aggregate data.

Recommend adding a modern data collection stage.

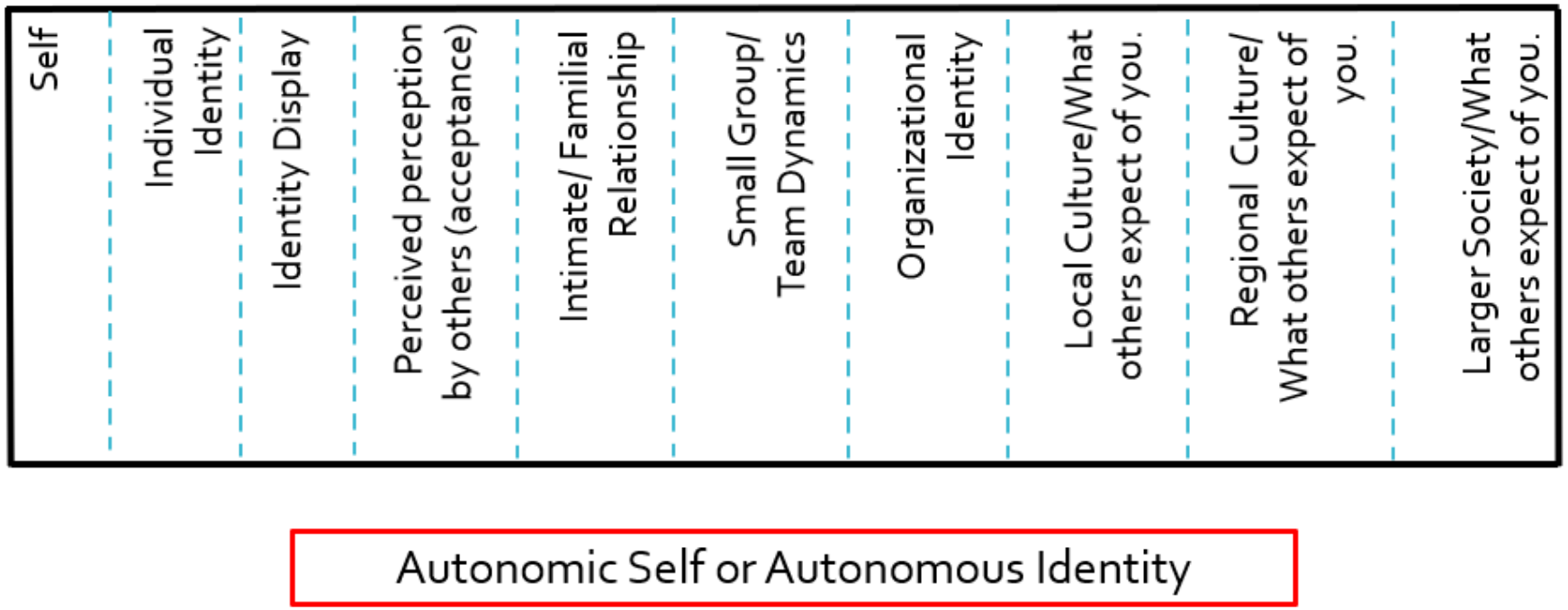


Recognition that an organization may not "create" its own data.

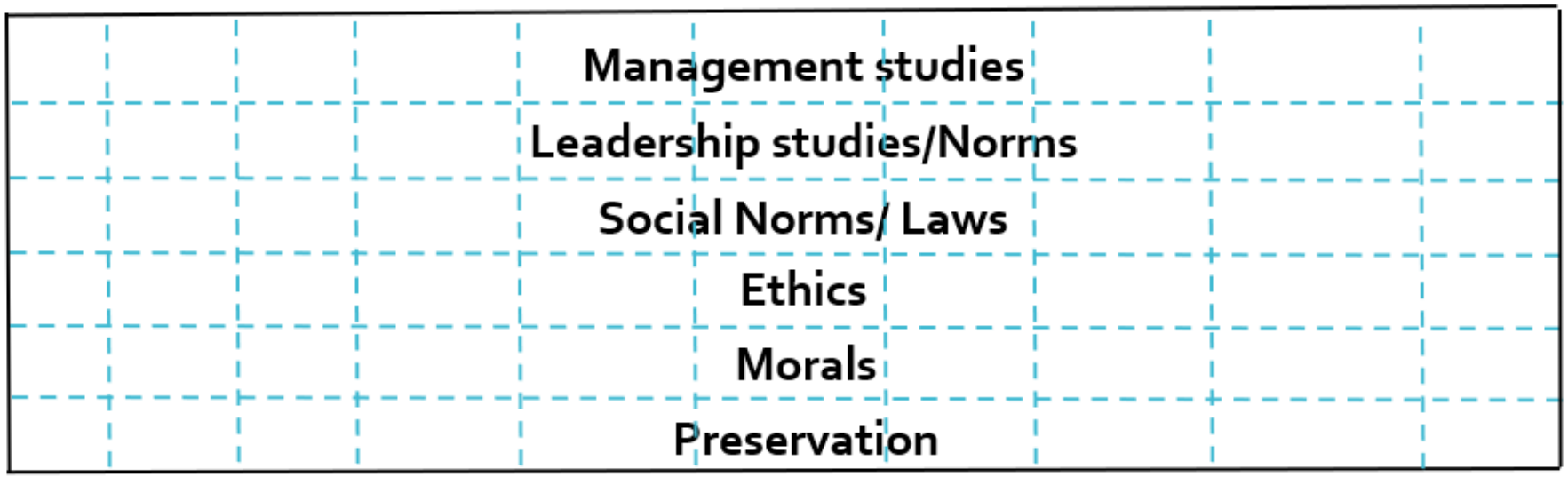
Technology component to component level security



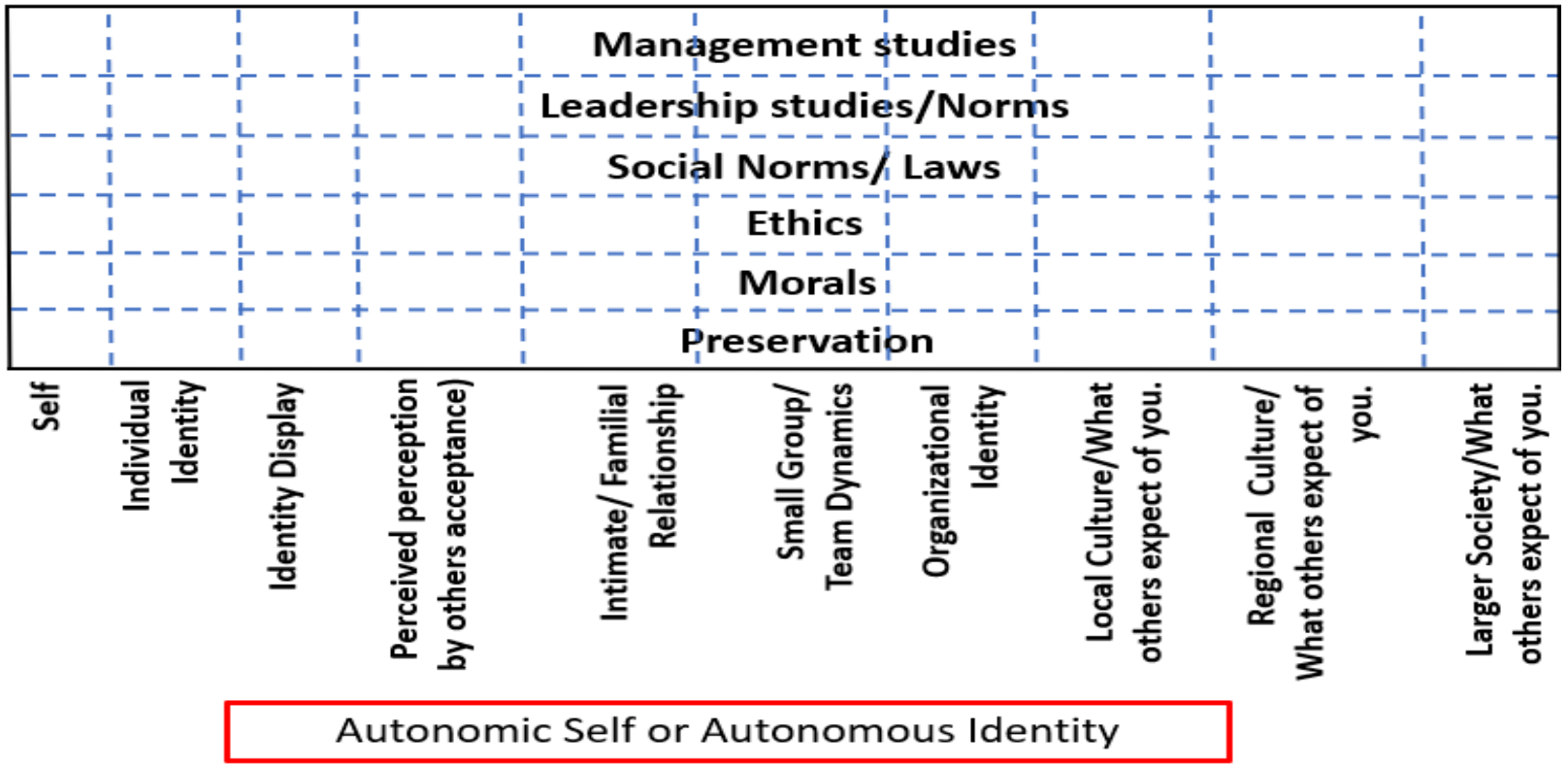
People Countermeasure (part 1)



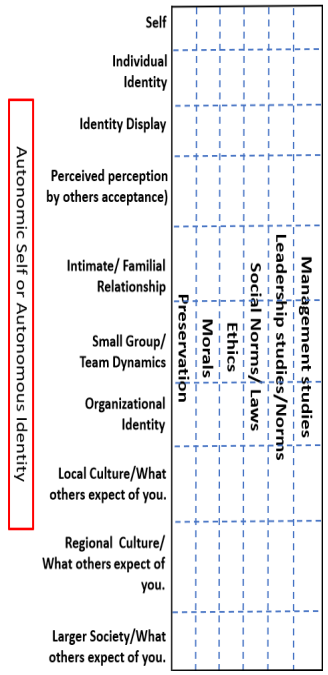
People Countermeasure (part 2)



People Countermeasure (Combined and Overlaid)



People Component Level Security Countermeasure Implications



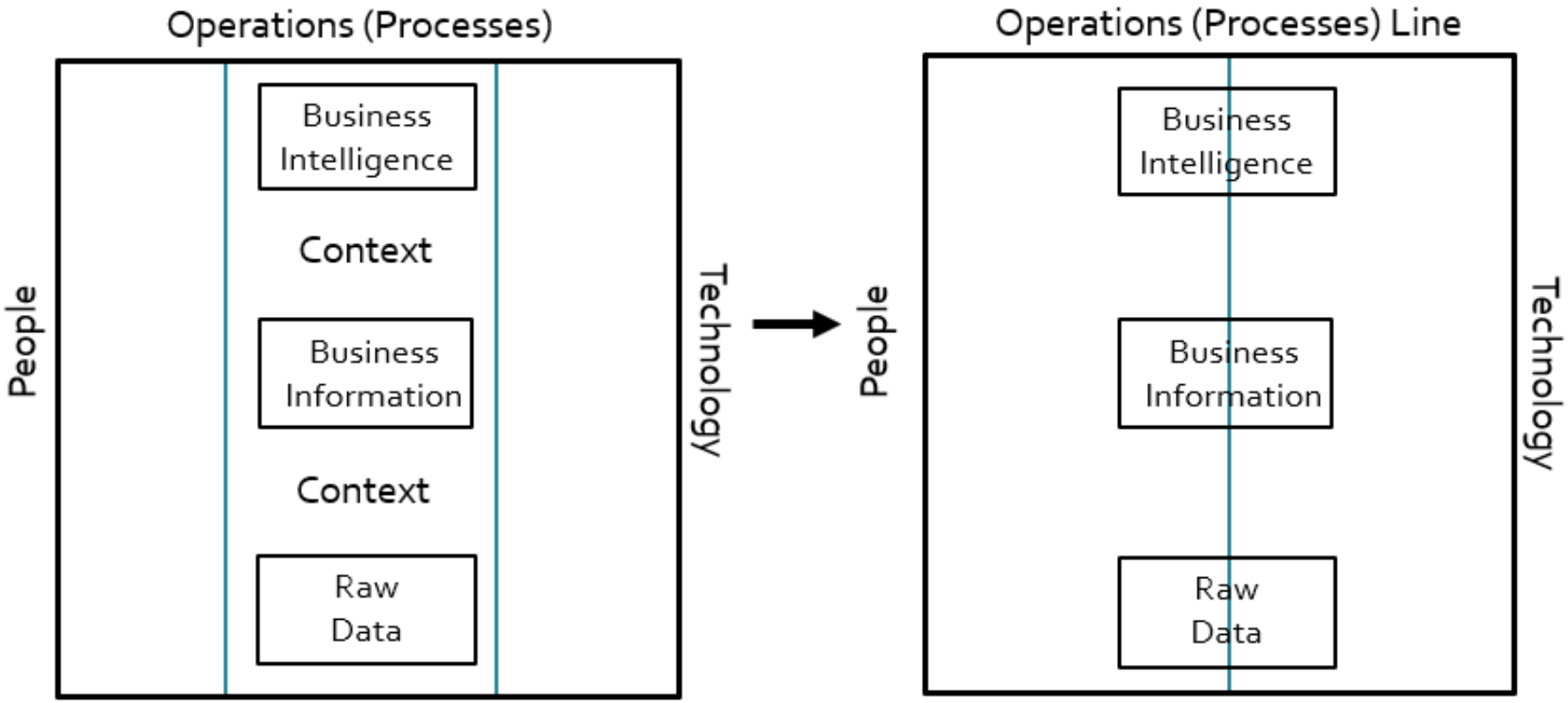
Some adjoining career fields which can be brought into Cybersecurity by adding adversarial thinking training to existing knowledge paths:

- Psychology
- Sociology
- Anthropology
- Leadership Studies
- Managerial Studies
- Cultural Studies

Process Component Level Security Countermeasure Implications

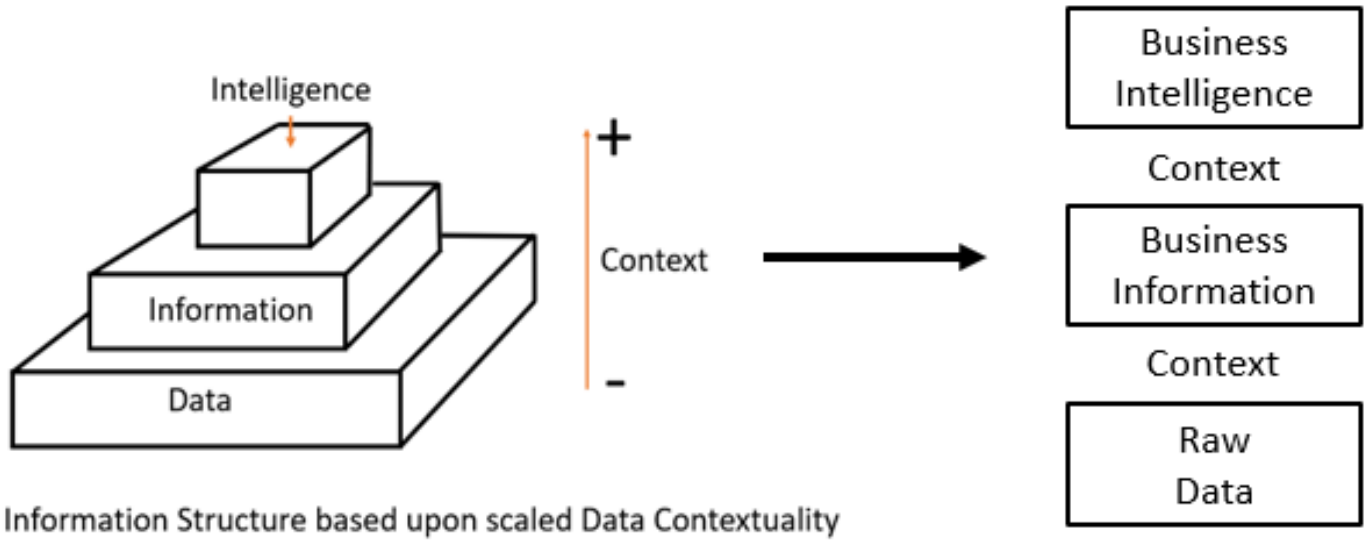
- Processes are an extension of either:
  - People skills
  - Technological capabilities
- They are the direct interaction of people and technology
- Intersection creates a *Technology capability and people skills line or process line*

Understanding Process Component Level Security Countermeasure Implications



Why add context?

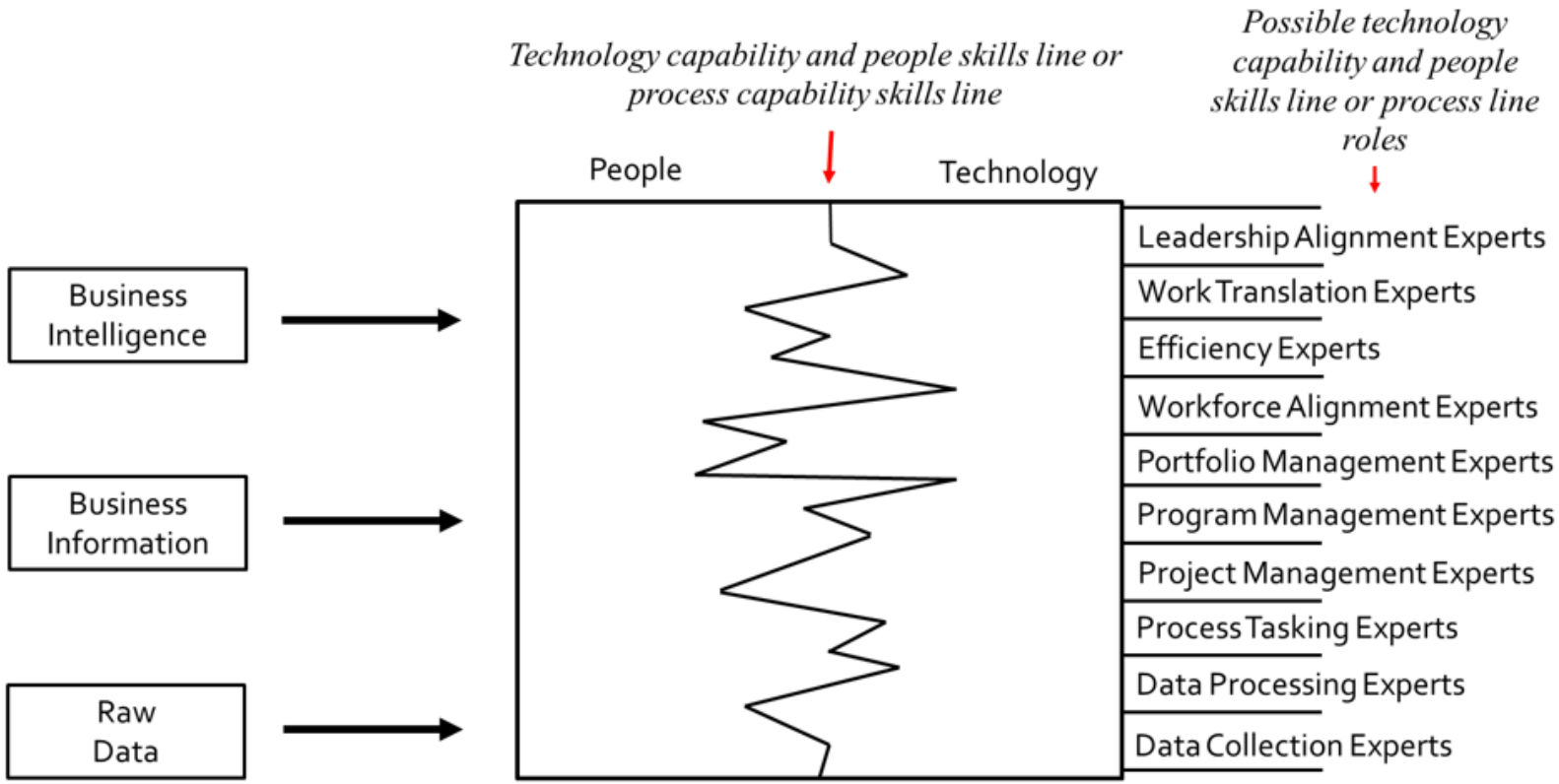
Because context is the answer to both operational and strategic business questions.



Note: Information Structure based upon scaled Data Contextuality

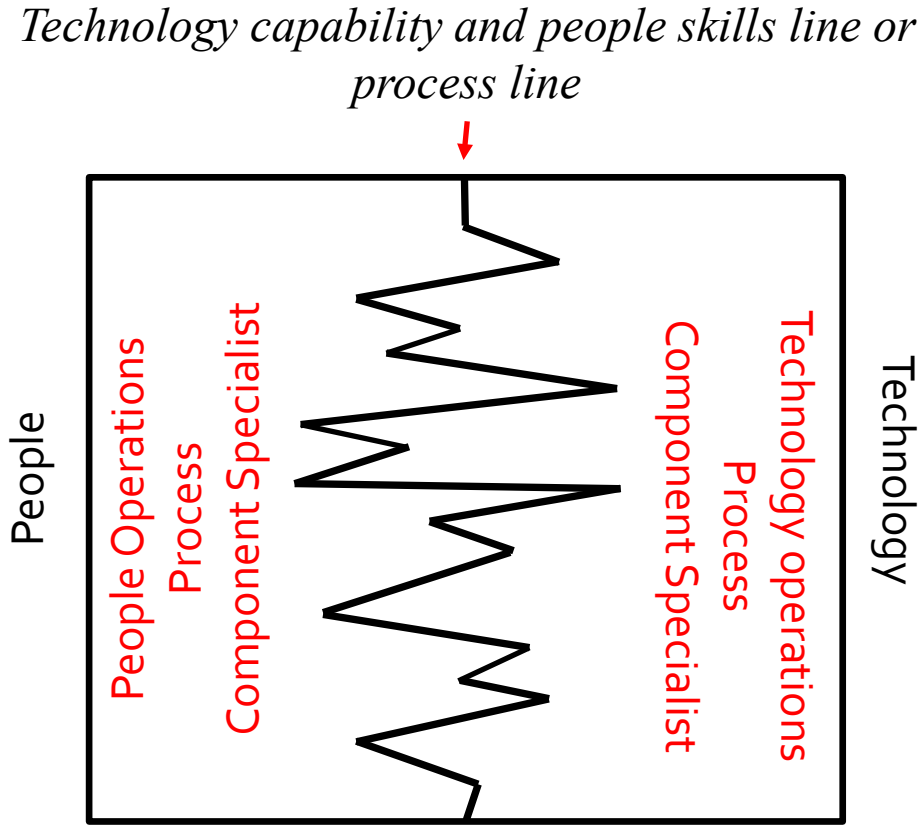
Context ties data to our stated business need, if it isn't stated (or asked) you cannot reasonably respond to it.

Breaking down the processes categorization



We have preexisting job specialization categories – but are we wisely integrating them?

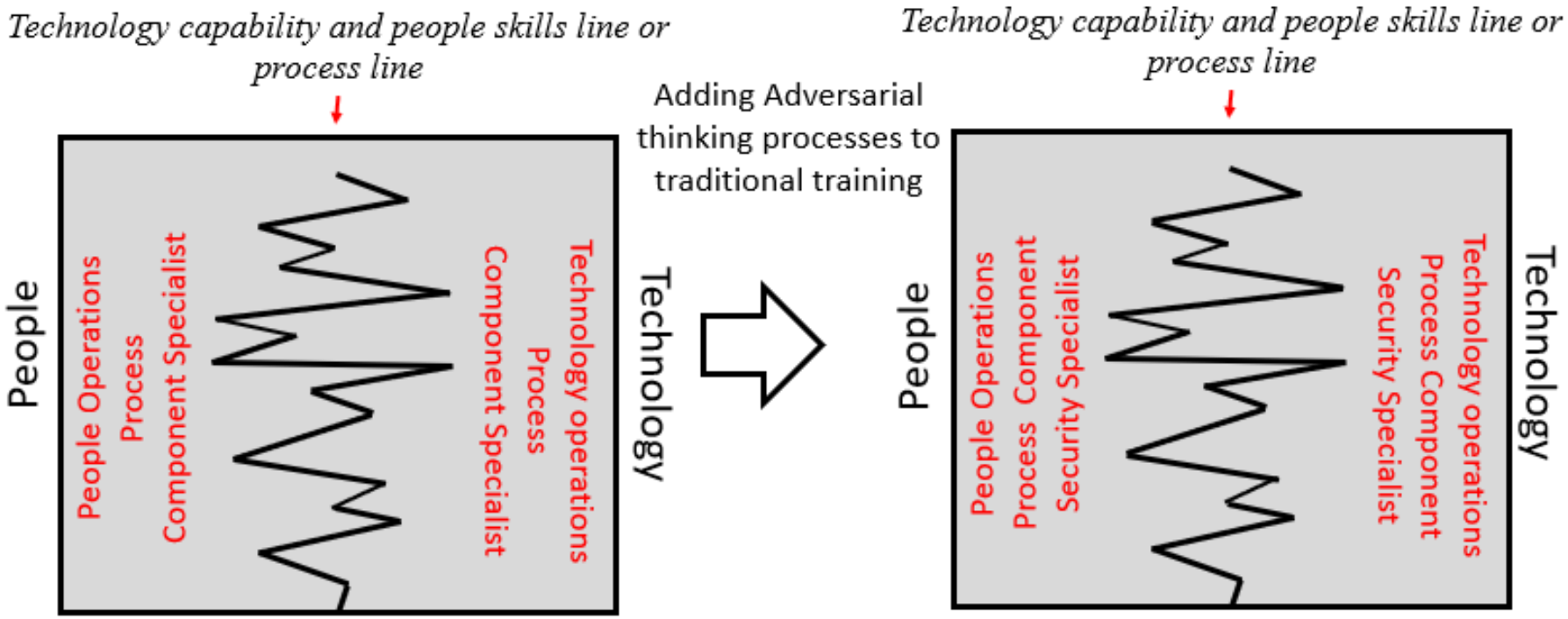
Operations Process Component Specialists



To make existing fields cyber(security) – just add adversarial thinking.

- Adversarial thinking is essentially a recognition of a risk and "why" it is important.
- Add adversarial thinking to normally recognized training.
- Operations Process Component Specialists to Operations Process Component Security Specialists.

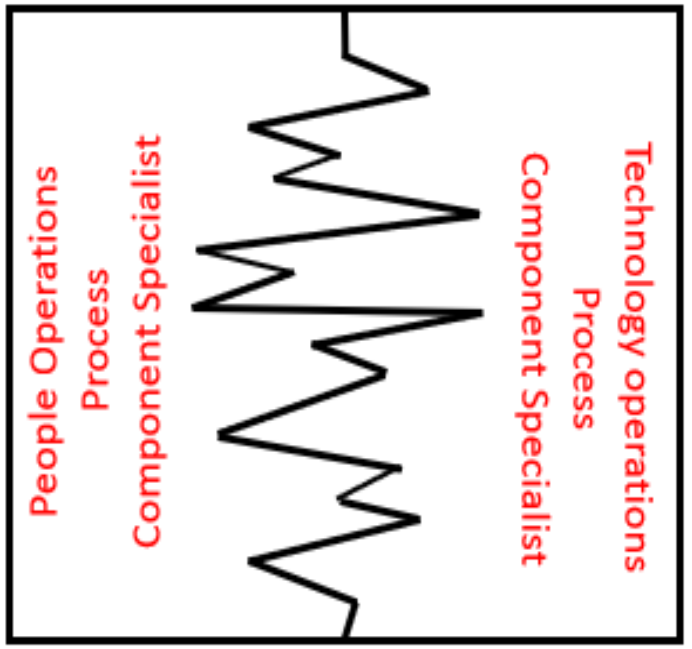
Operations Process Component Specialists



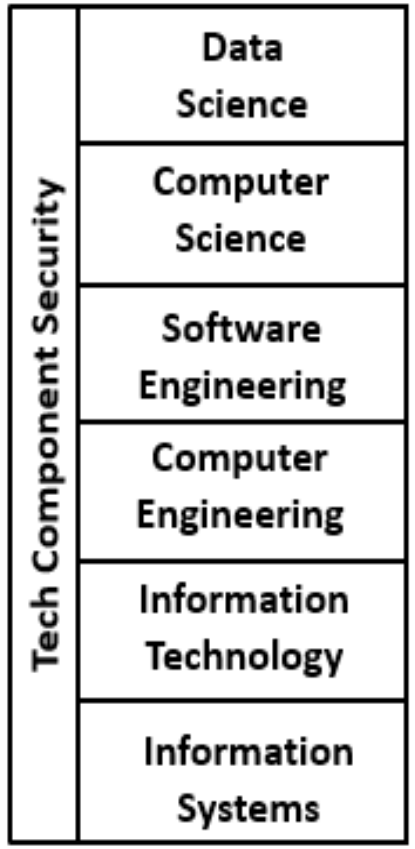
Putting it all together

+

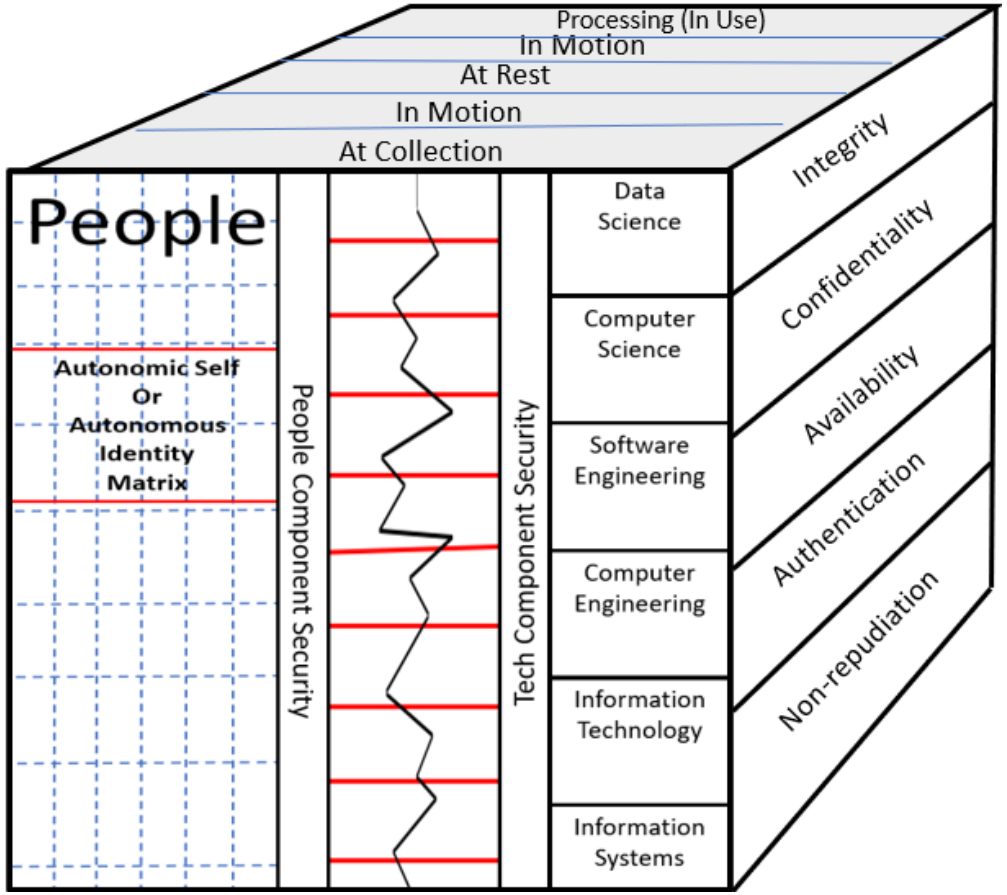
Technology capability and people skills line or process line



+



Presenting the new recommended model and vantage point



Some quick definitions to build on:

- Who = People Countermeasure
- How = Processes Countermeasure
- What = Technology Countermeasure
- Why = The underlying logic as to why an action is taken to reduce or eliminate a risk.

A simple test:

Who, How, OR What = Component skill

This translates to the People, Process, or Technology Countermeasure

Who, How, **OR** What = Component skills

\+ Why = Security

This translates to the People, Process, or Technology Countermeasure with an adversarial or countermeasure understanding

Who, How, AND What + Why = Cybersecurity

This translates to a holistic countermeasure viewpoint/approach with an adversarial or countermeasure understanding

Usage Cases #1

- A group of technicians study and learn how to properly deploy and secure firewalls, routers, and switches.

(Hint: don't read anything else into it, make no assumptions)

Solution #1

This is:

- IT Security

Usage Cases #2

- A programmers deploy websites based upon scope of work as requested by customers

(Hint: don’t read anything else into it, make no assumptions)

Solution #1

This is:

- Traditional Development

Usage Cases #3

- A Project Manager works with corporate risk management and identifies new corporate risks, based upon a new crypto-campaign from a foreign state. This campaign targets users who frequent online news channels.

(Hint: don't read anything else into it, make no assumptions)

Solution #1

This is:

- Cybersecurity

Thank you.
Questions?