Security and Technologies - Future Cyberskills -

Jeimy J. Cano M., Ph.D, CFE
Associate Professor
Universidad del Rosario
School of Business
COLOMBIA

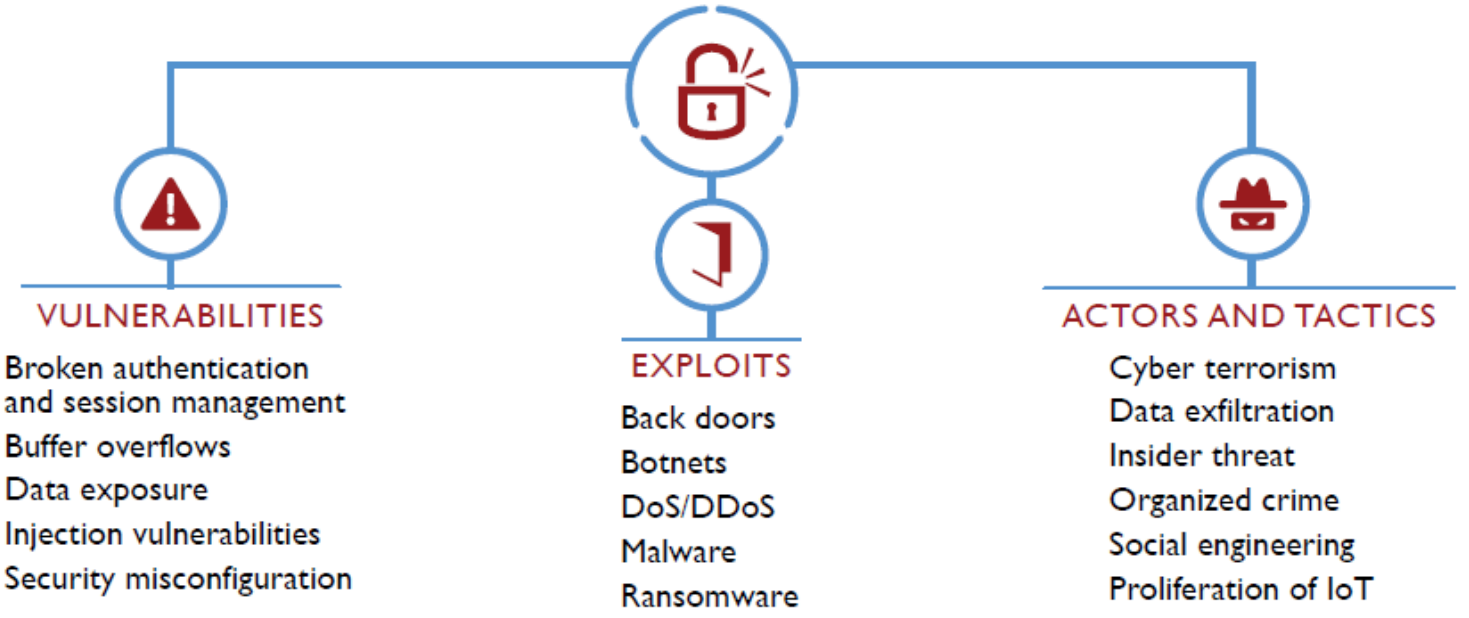
Agenda

- Introduction
- Current context
- InfoSEC & CyberSEC fundamentals
- InfoSEC evolution
- Cybersecurity: Educative and Corporate challenges
- Emergent challenges
- Conclusions

Introduction

Issues of major concern

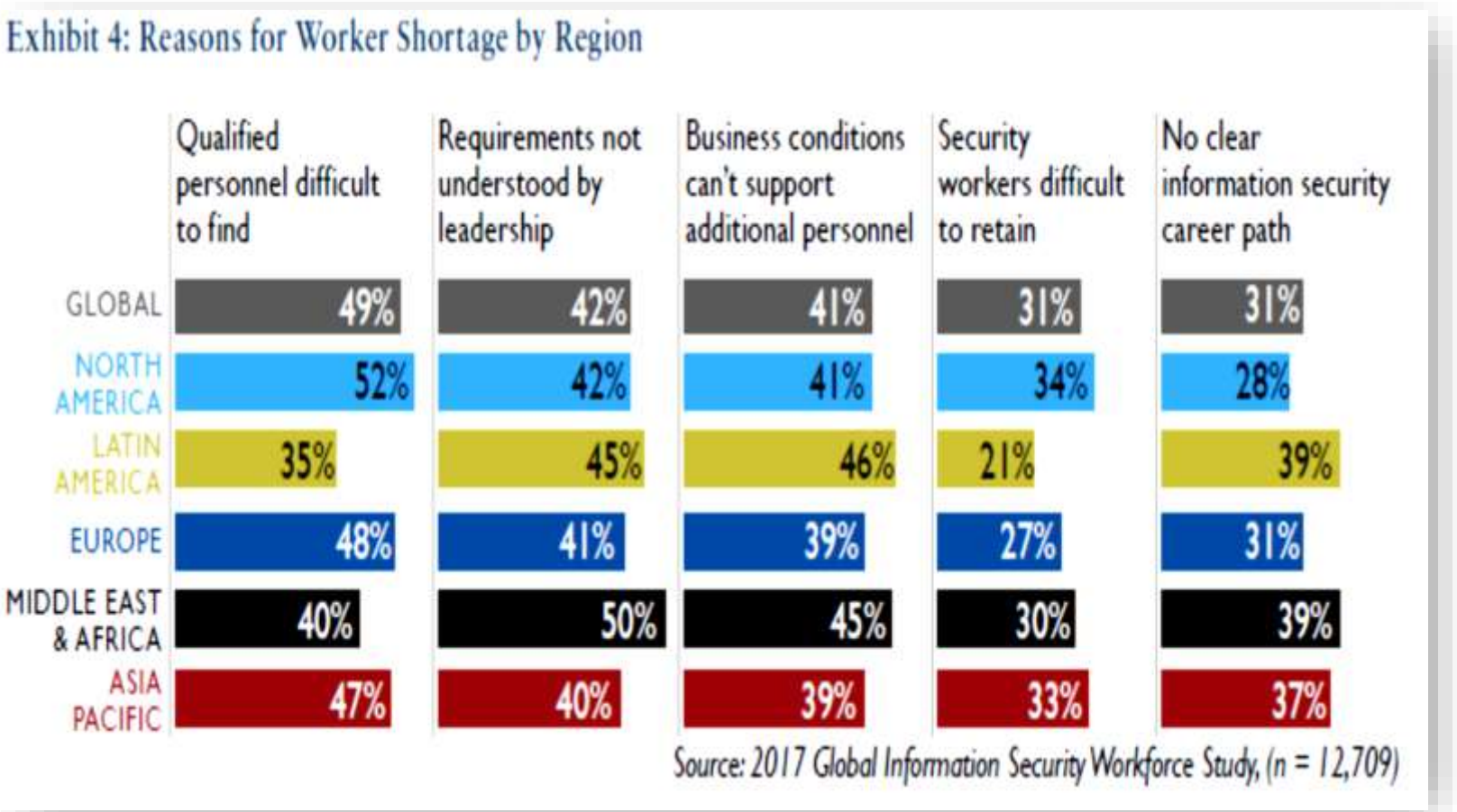
Exhibit 1: Threats of Most Concern



Source: 2017 Global Information Security Workforce Study

Source: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

Deficit of professionals in both InfoSec and CiberSec



Source: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

Professionals in both InfoSec and CiberSec

Europa

Latin America

Source: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

Current Context

Global CEO Priorities

Terrorism and cyber threats rise

Q Considering the following threats to your organisation's growth prospects, how concerned are you about the following?

	2017		2018
1	42% Over-regulation		Over-regulation 42%
2	34% Uncertain economic growth		Terrorism 41%
3	31% Exchange rate volatility		Geopolitical uncertainty 40%
4	31% Availability of key skills		Cyber threats 40%
5	31% Geopolitical uncertainty		Availability of key skills 38%
6	29% Speed of technological change		Speed of technological change 38%
7	29% Increasing tax burden		Increasing tax burden 36%
8	26% Changing consumer behaviour		Populism 35%
9	24% Social instability		Climate change and environmental damage 31%
10	24% Cyber threats		Exchange rate volatility 29%

Chart shows percentage of respondents answering **'extremely concerned'**.

Source: PwC, 21st Annual Global CEO Survey © 2018 PricewaterhouseCoopers LLP. All rights reserved.

Source: https://www.pwc.com/gx/en/ceo-survey/2018/pwc-ceo-survey-report-2018.pdf

Ciber risk definition

Source	Definition
Mukhopadhyay et al. (2005, 2013)	Risk involved with malicious electronic events that cause disruption of business and monetary loss
Böhme and Kataria (2006)	Breach or failure of information systems
Cebula and Young (2010)	Operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems
Kshetri (2010)	A cybercrime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules, or regulations.
Ogut et al. (2011)	Information security risk
The UK Cyber Security Strategy (2011)	Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.
World Economic Forum (2012)	"Cyber risks" are defined as the combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation.
World Economic Forum (2012)	"Cyber" refers to the interdependent network of information technology infrastructures, and includes technology "tools" such as the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
Hua and Bapna (2013)	Cyber terrorism: Attacks implemented by cyber terrorists via information systems to (1) significantly interfere with the political, social or economic functioning of a critically important group or organization of a nation, or (2) induce physical violence and/or create panic.
National Association of Insurance Commissioners (2013)	Defines cyber by providing typical examples: Identity theft, business interruption, damage to the firm's reputation, disclosure of sensitive information and business interruption
National Institute of Standards and Technology (NIST, 2013)	Defines cyber space as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."
Tallinn Manual (Schmitt, 2013)	Cyberspace: The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks.
Willis (2013a)	Cyber risk can be defined as the risk connected to activity online, internet trading, electronic systems and technological networks, as well as storage of personal data
Swiss Re (2014)	Any risk emanating from the use of electronic data and its transmission. This encompasses physical damage caused by cyber-attacks, loss or corruption of data and its financial consequences, fraud committed by misuse of data, as well as any liability arising from a failure to maintain the availability, integrity, and confidentiality of electronically stored information – be it related to individuals, companies, or government. In this context, cyber risk insurance addresses the first and third party risks associated with e-business, the internet, networks and informational assets.
CRO Forum (2014)	Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or government.
Institute of Risk Management (2014)	Any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.
Refsdal, Solhaug, and Stolen (2015)	Definition consisting of three elements: -A cyber-risk is a risk that is caused by a cyber-threat -A cyber-threat is a threat that exploits a cyberspace -Cyberspace is a collection of interconnected computerized networks, including services, computer systems, embedded processors, and controllers, as well as information in storage or transit.
Lloyds (2015)	Losses relating to damage to, or loss of information from, IT systems and networks.
Lloyd's (2015a)	Definition of Cyber-Attack: exposures arising from a malicious electronic act which for the purpose of this bulletin we label as 'cyber-attack'. Cyber-attack is therefore the proximate cause of loss, although the consequences may include property damage, bodily injury, financial loss or other forms of damage.
CRO Forum (2016)	Cyber risk [is] defined as the risk of doing business in the cyber environment. The definition of cyber risk covers: • Any risks emanating from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. • physical damage that can be caused by cyber attacks. • fraud committed by misuse of data. • any liability arising from data use, storage and transfer, and • the availability, integrity and confidentiality of electronic information be it related to individuals, companies or government.

Souce: Eling, M. & Schnell, W. (2016) What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*. 17(5). pp.474-491. Doi: https://doi.org/10.1108/JRF-09-2016-0122. Online-Appendix 3

Cyber risk

Key elements

Not authorized activity:

Actions intentionally or unintentionally committed in the context of the organization..

Offender:

State and non-state actors, organized crime, internal employees, digital mercenaries

Vulnerability:

Determined by the practices and standards that the organization has on information technology management, its processes and people.

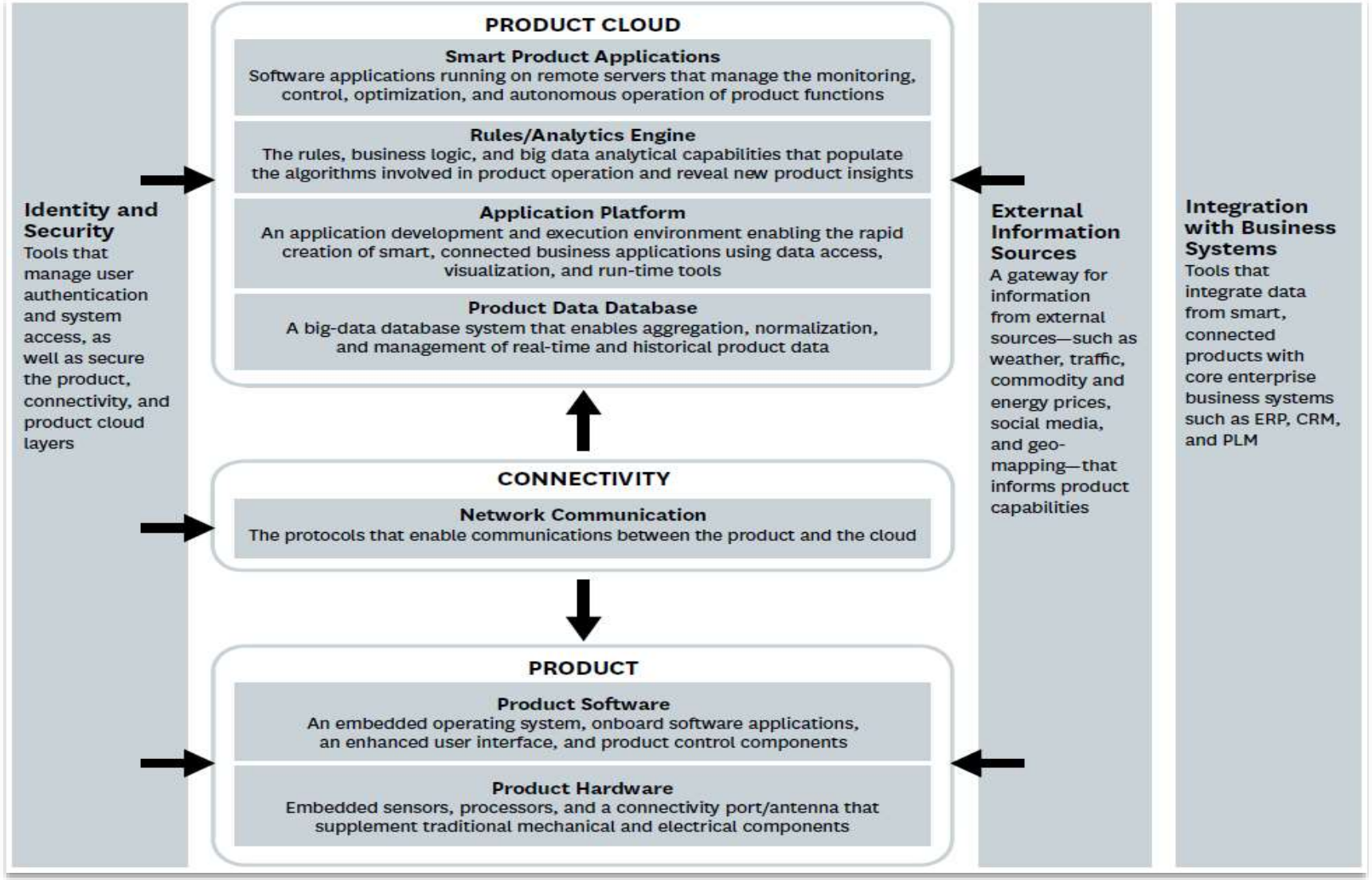
Attack:

Exploiting known or unknown vulnerabilities to perform actions that disrupt, deteriorate, alter, reveal or destroy key business assets and/or services. E.g: Malware, DDos.

Consequence:

The effects are generated based on the attackers' intentions. E.g.: Disclosure of information, espionage, extortion, theft of information, sabotage, fraud..

Products/Services digitally modified



Porter, M. y Heppelmann, J. (2014) How Smart, connected products are transforming competition. *Harvard Business Review*. Noviembre.p.7

Types of attackers

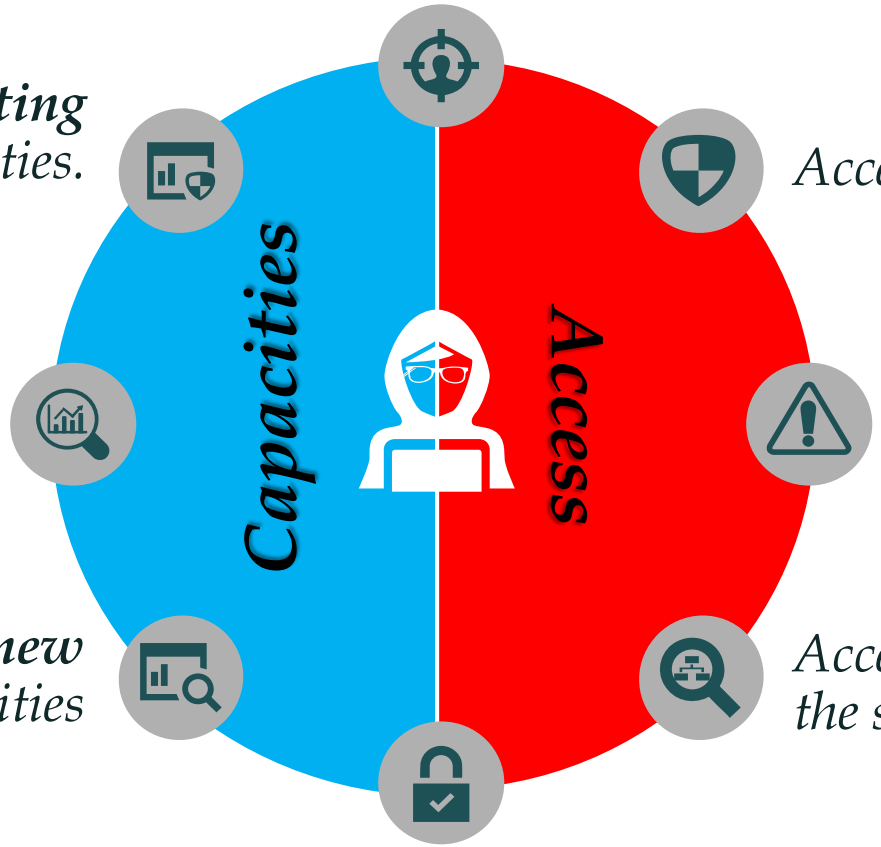
Based on type of access and its capabilities

Vulnerabilities

*Those who only **execute existing** attacks with known vulnerabilities.*

*Those who can scan a system for **new vulnerabilities** and **develop code to exploit them**.*

*Those who **create new** vulnerabilities*



Access to physical hardware

Access to software or data

Access to people who use or run the system

Assumptions falsification

Based on: DoD (2013) Resilient Military Systems and the Advanced Cyber Threat. *Task Force Report*. Defense Science Board. January. Recuperado de: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

Cyber insurance & its challenges

Figure 6. Costs of a data breach

Above the surface: Well-known cyber incident costs

1. Customer breach notifications
2. Post-breach customer protection
3. Regulatory compliance (fines)
4. Public relations/crisis communications
5. Attorney fees and litigation
6. Cybersecurity improvements
7. Technical investigations

Below the surface: Hidden or less visible costs

1. Insurance premium increases
2. Increased cost to raise debt
3. Operational disruption or destruction
4. Lost value of customer relationships
5. Value of lost contract revenue
6. Devaluation of trade name
7. Loss of intellectual property

Source: "Beneath the surface of a cyber attack: A deeper look at business impacts," Deloitte Cyber Risk Services.

Deloitte University Press | dupress.deloitte.com

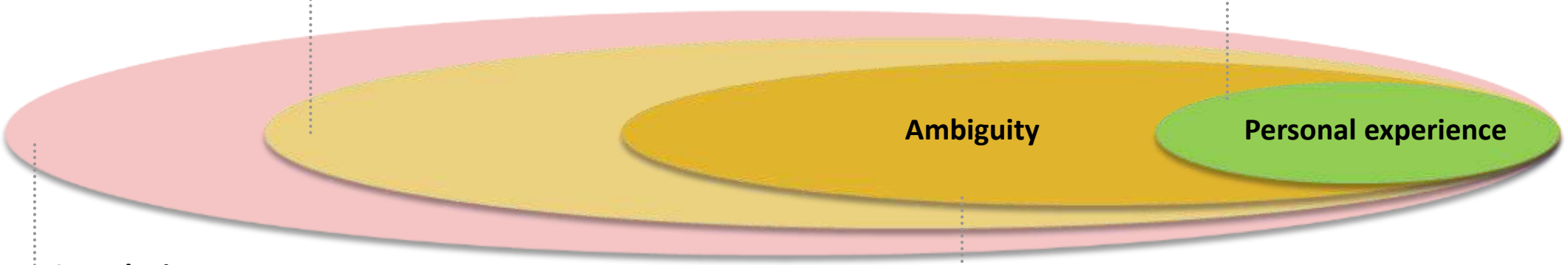
Fuente: https://www2.deloitte.com/insights/us/en/industry/financial-services/demystifying-cybersecurity-insurance.html

InfoSEC & CiberSEC Fundamentals

Understanding risk in digital context

Uncertainty
A state of indetermination between a cause and its effects.

The particular history of each individual interpreted in the secret chamber of his assumptions.



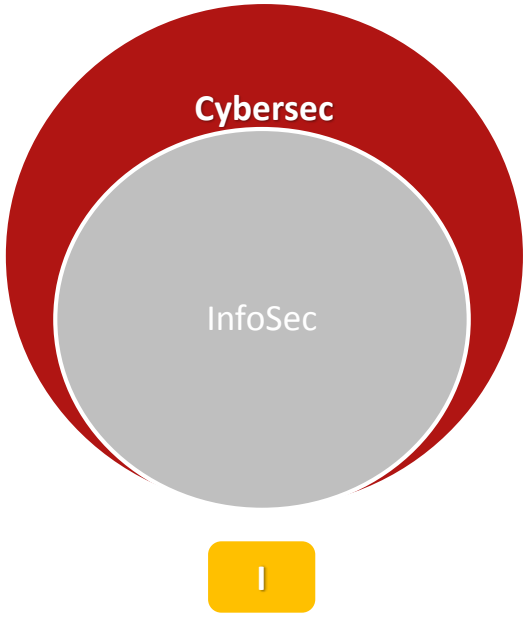
Complexity
The result of the limited ability to distinguish specific aspects of reality that go beyond the previous knowledge of the observers.

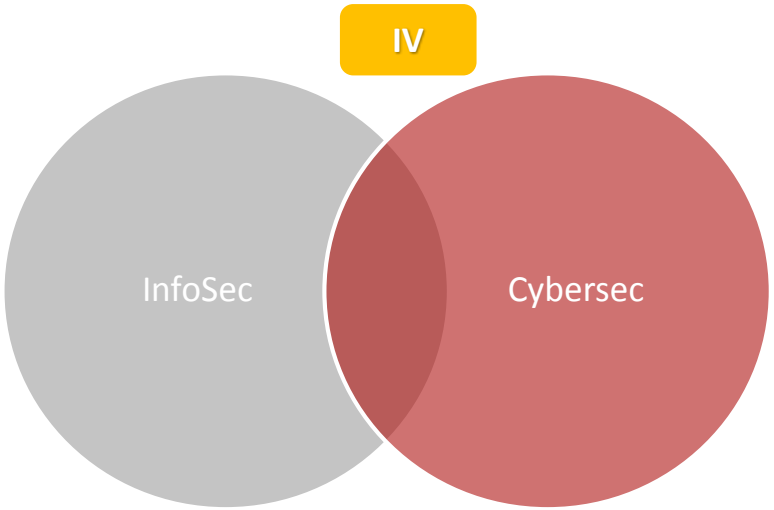
It is the result of legitimate interpretations based on socially accepted meanings and real facts.

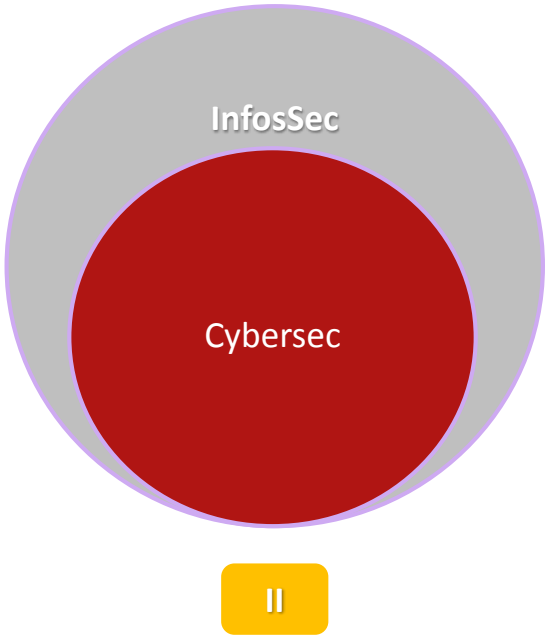
Risk: *A situation or event where something of human value is at stake and where the outcome is uncertain*

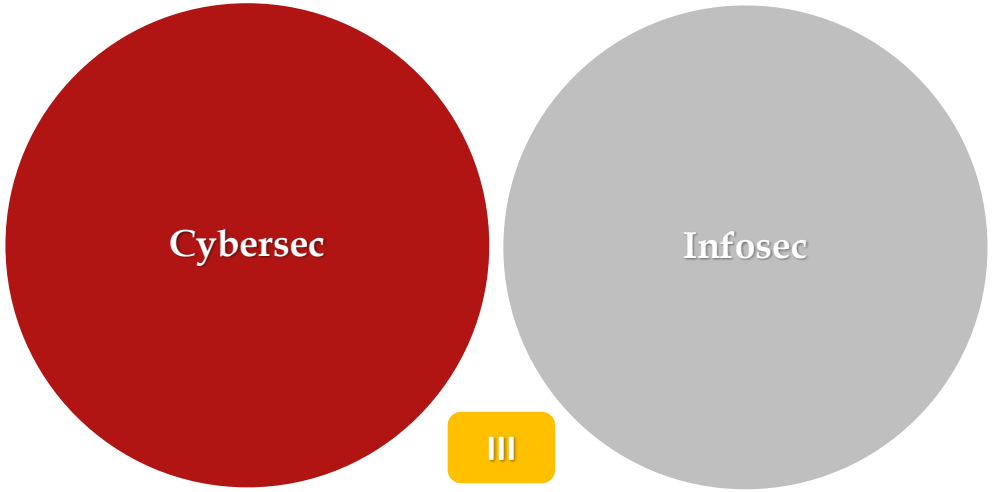
Based on: Rosa, E., Renn, O. y McCright, A. (2014) *The risk society revisited. Social theory and governance*. Philadelphia, Pennsylvania. USA: Temple University Press.

InfoSEC Vs CiberSEC

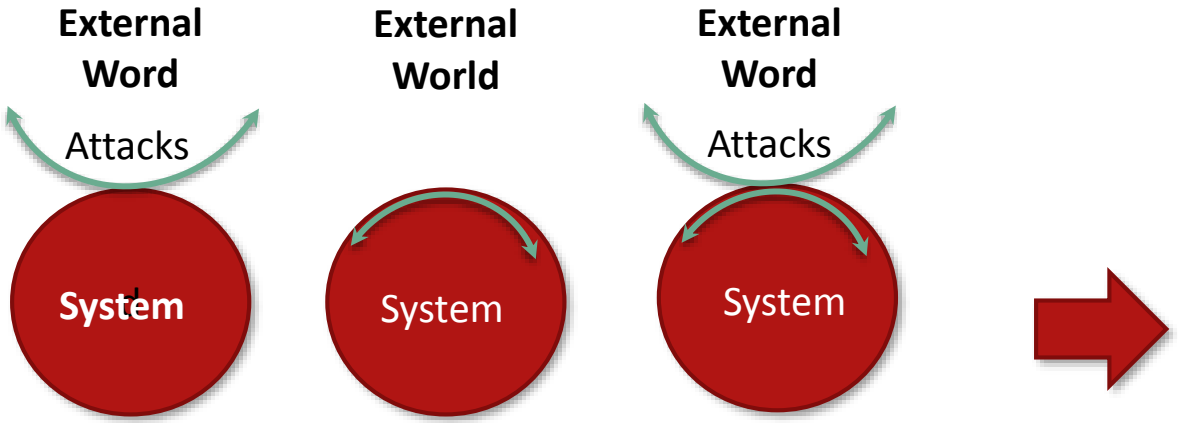








Conceptual notes about cybersec



Security

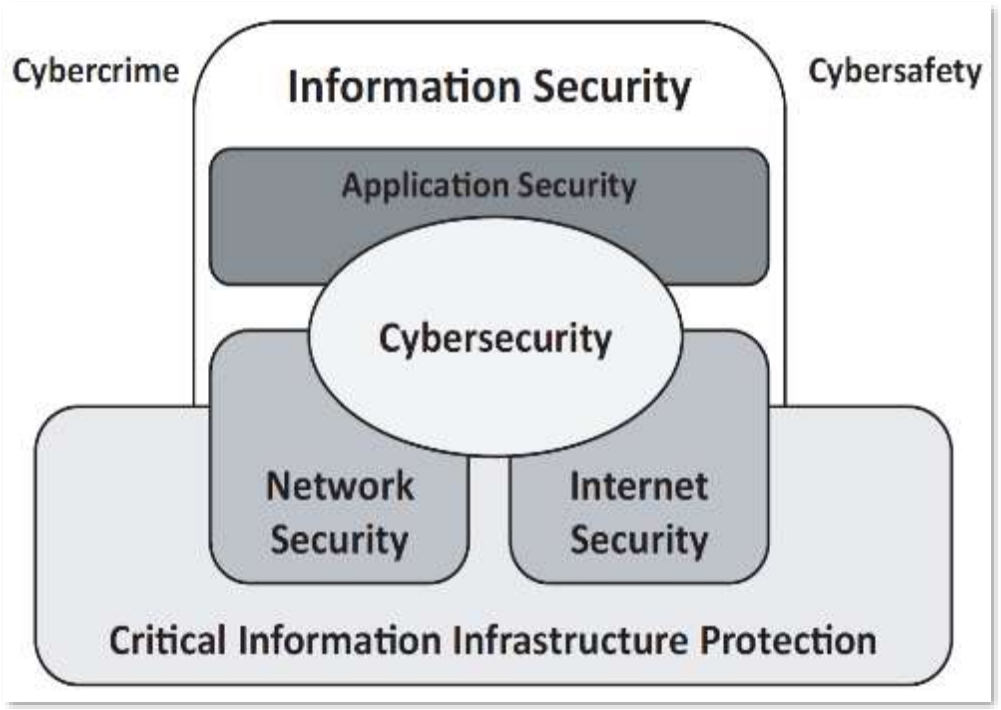
"Avoiding external world affects the system"

Safety

"Avoid the system affects external world"

Security+Safety

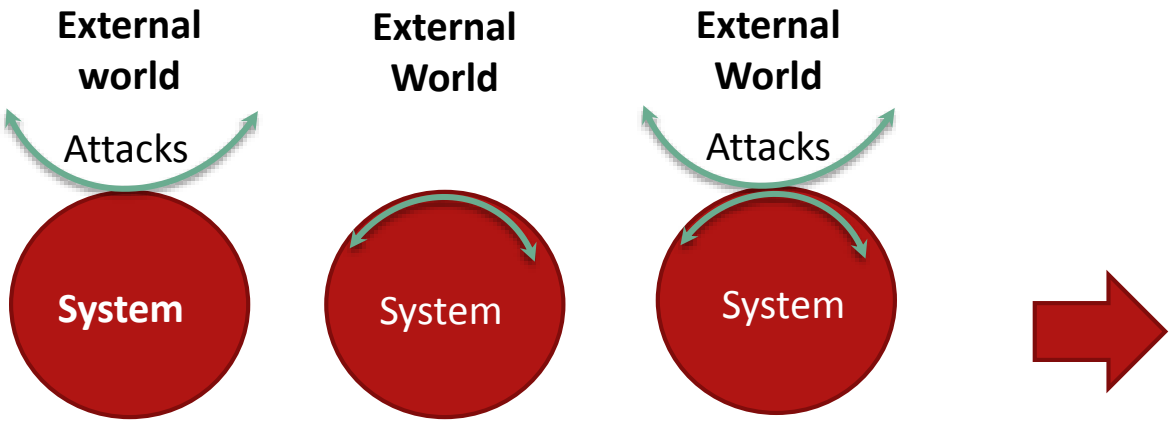
"Ensure that the system continues to operate, without affecting the outside world, despite the attacks"



From: ISO 27032 – Information Technology- Security Techniques – Guidelines for cybersecurity.

Source: ALXELROD, W.C (2013) *Engineering Safe and Secure Software Systems*. Artech House

Conceptual notes about Cybersec



Security

"Avoiding external world affects the system"

Safety

"Avoid the system affects external world"

Security+Safety

"Ensure that the system continues to operate, without affecting the outside world, despite the attacks"

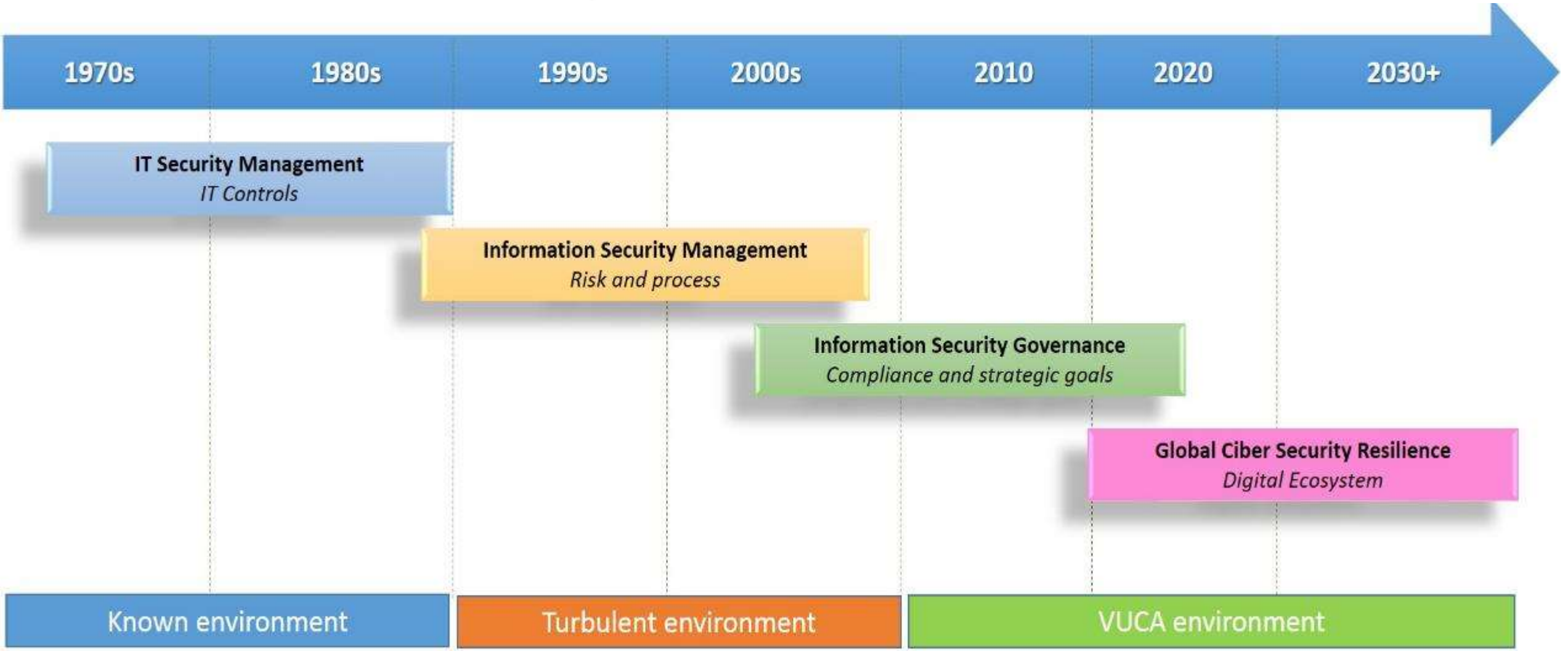
Source: ALXELROD, W.C (2013) *Engineering Safe and Secure Software Systems*. Artech House

Enterprise Cybersecurity

It is an ***enterprise capacity*** defined to defend and anticipate the digital threats inherent to the ecosystem where the organization operates, in order to protect and ensure the resilience of the operations and the reputation of the company.

InfoSEC Evolution: From practices to capabilities

InfoSEC Evolution



Definitions: Practices & Capacity

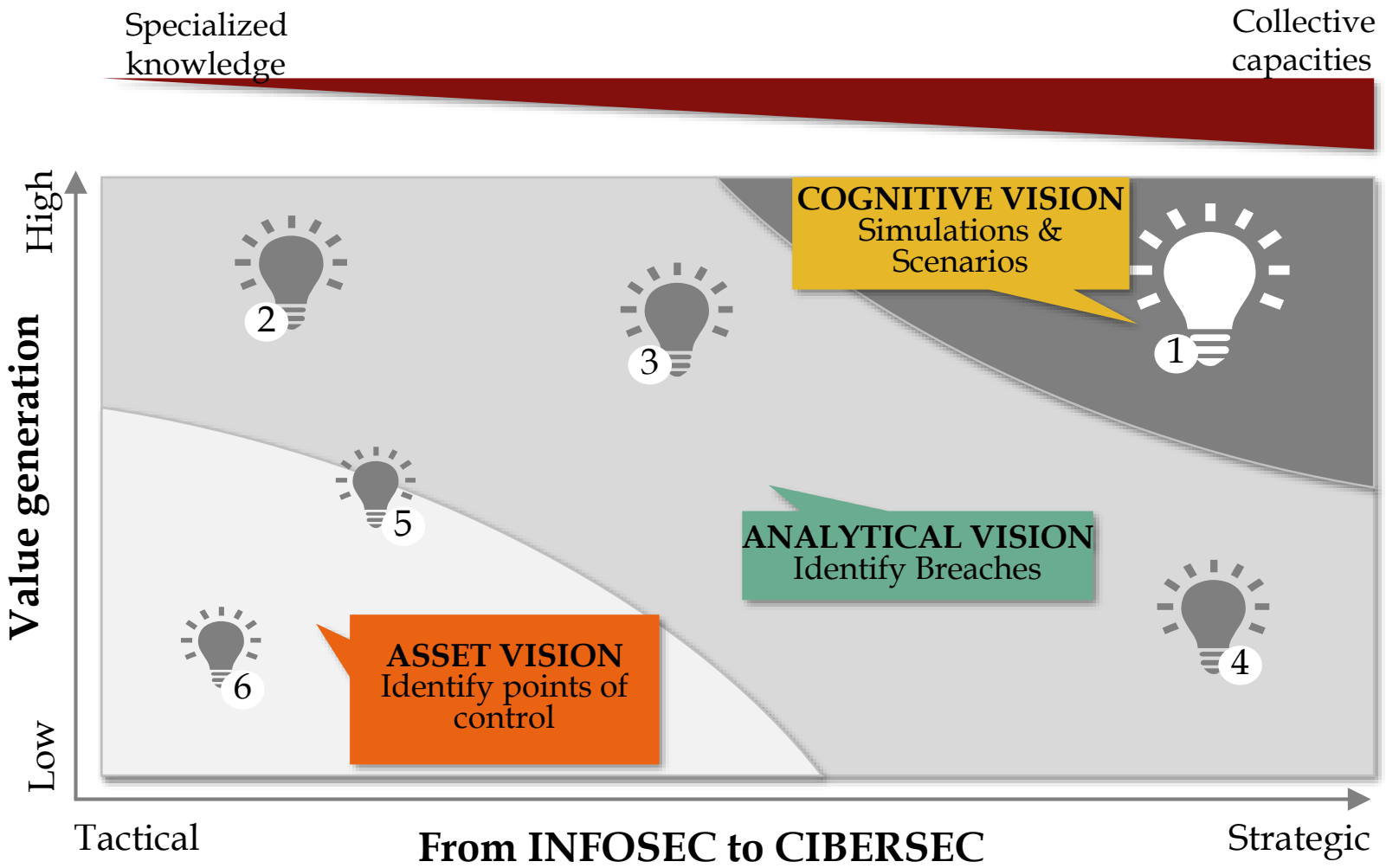
Characteristics

- Applied and tested bodies of knowledge
- Based on **certainties**
- Verifiable and auditable
- **Risk: It is a threat**

Characteristics

- Develops learning
- Based on **uncertain and ambiguous scenarios**.
- Challenge previous knowledge and **develop new distinctions**
- **Risk: An opportunity**

Evolution: security & control practices



1. War games
2. Social engineering exercises
3. Intelligence and Threat hunting
4. Infosec risk analysis
5. Infosec Audit
6. Vulnerability analysis

INFOSEC practices & CIBERSEC capacities

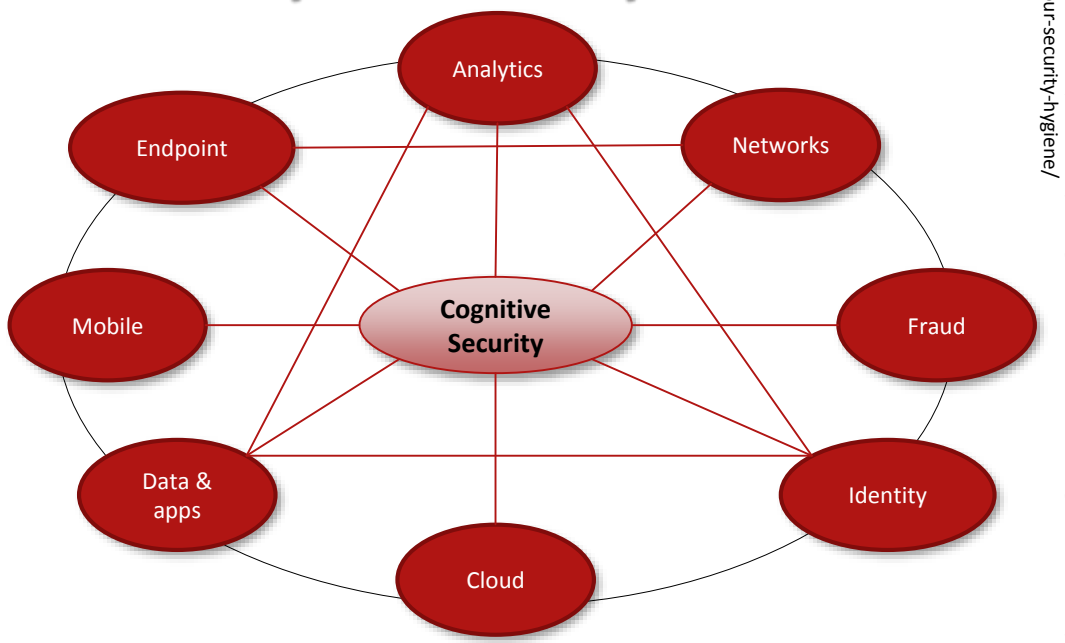
Security domains

Enpoint security	Network security	Data security
Security communication	Management vulnerabilities	Software security
IT controls management	Identity management	Mobile security

Protection & assurance

Practices

Cybersec Ecosystem



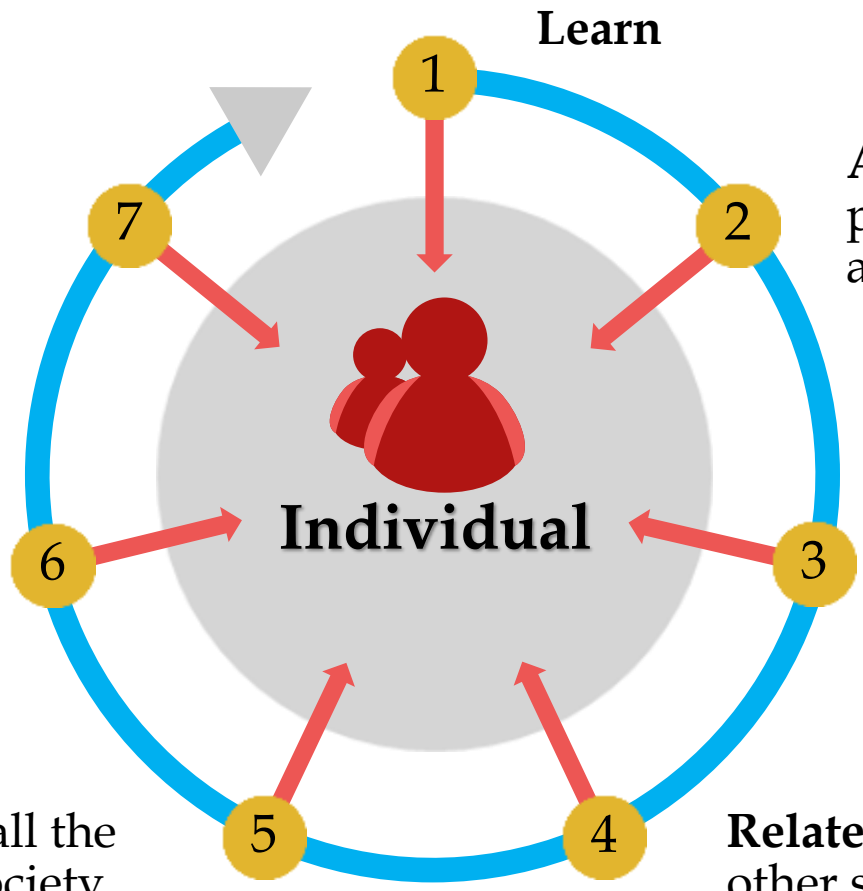
Defend & anticipate

Capacities

Adaptado de: Falco, C. (2016) Unleashing the Immune System: How to Boost Your Security Hygiene. Recuperado de: https://securityintelligence.com/news/unleashing-the-immune-system-how-to-boost-your-security-hygiene/

CiberSEC:
Educative & Corporate challenges

Education objetives in current context



Disconnect known concepts and rethink them in unknown scenarios.

Anticipate and solve new problems, creating alternative solutions.

Thinking in an interdisciplinary and holistic way, to perceive the dimensions of the challenges

Identify key information and transform it into knowledge.

Read and communicate in all the media generated by the society.

Relate learning to reality and other sciences.

Adapted from: García, L., Ruiz, M. y García, B. (2009) *Claves para la educación. Actores, agentes y escenarios en la sociedad actual*. Madrid, España: Narcea-UNED. P.272

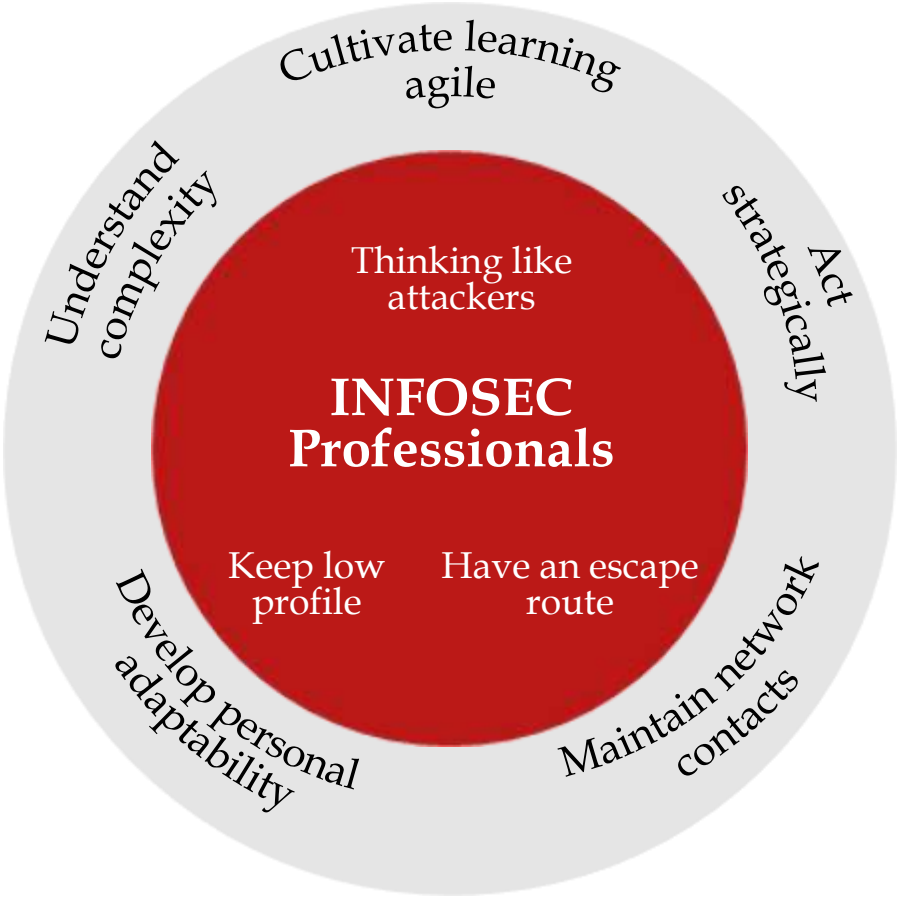
General concept of security

	Reference object	Value at risk	Threat source	Remarkable example of risk
National security (Militar & Political dimension)	The Nation	Sovereignty, territorial integrity	Other nations, terrorism	Extreme groups
Society security	Social groups	National Union, identity	Nations, foreign cultures, immigrants	Displaced by conflict
Human security	Individuals, humanity	Survival, quality of life	State, globalization, nature, terrorism	Natural disasters
Enviromental security	Ecosystem	Sustainability	Humanity	Global warming
Information security	People, process & technology	Trust	Human, technical and process vulnerabilities	Loss and/or leakage of information
Cibersecurity	Digital ecosystem	Resilience, governance	Estados, terrorismo, actores no estatales	Attacks on critical national infrastructure

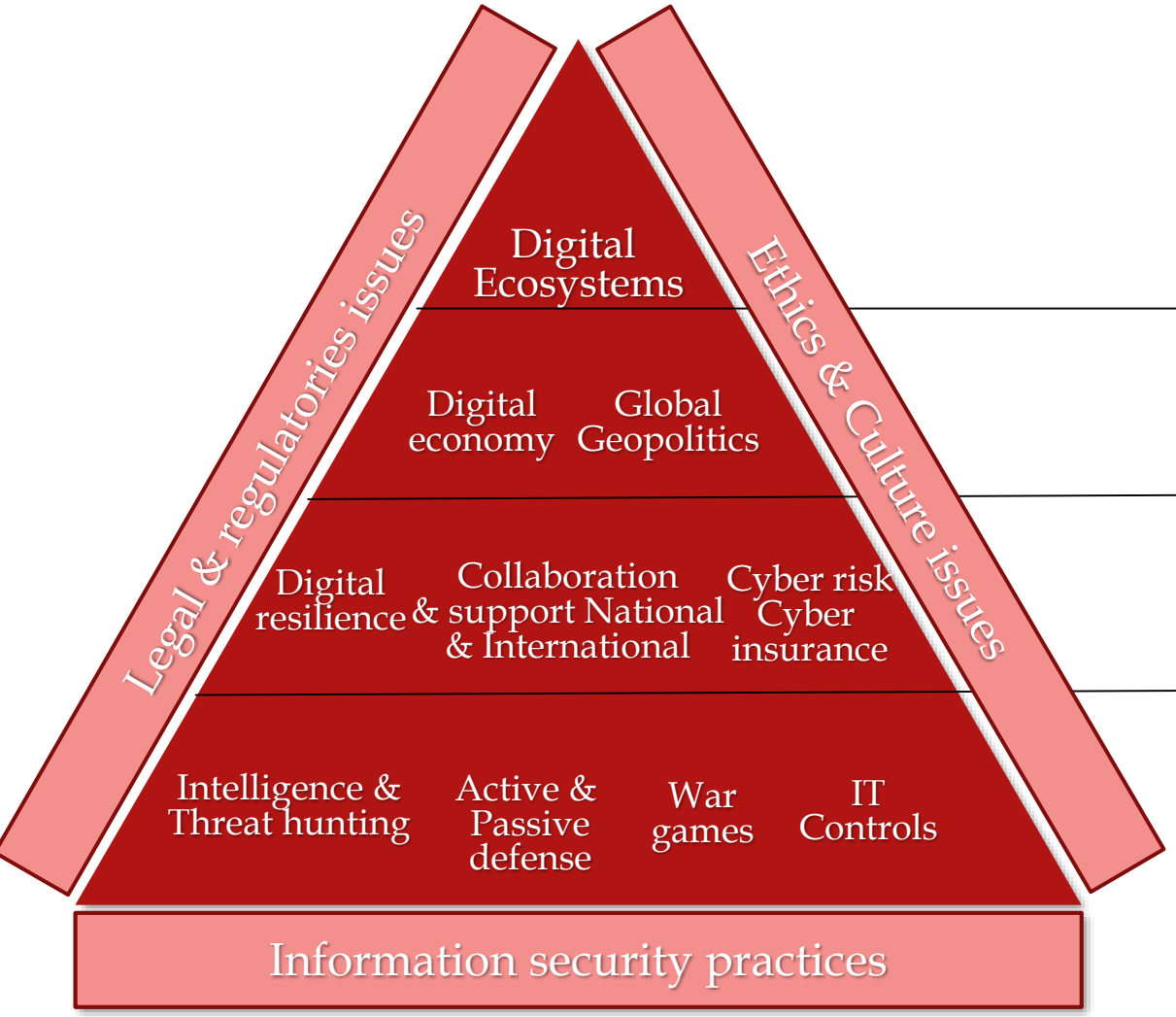
Adapted from: Gunter, H. (2005) *Threats, challenges, vulnerabilities and risks in enviromental and human security*. UNU Institute for Environment and Human Security (UNU-EHS). Publication Series of UNU-EHS. No.1. p.19. Recuperado de: http://collections.unu.edu/eserv/UNU:1868/pdf4040.pdf

INFOSEC Professionals – Key Skills

- Key skills
- Basic practices



CIBERSEC Professionals – Education



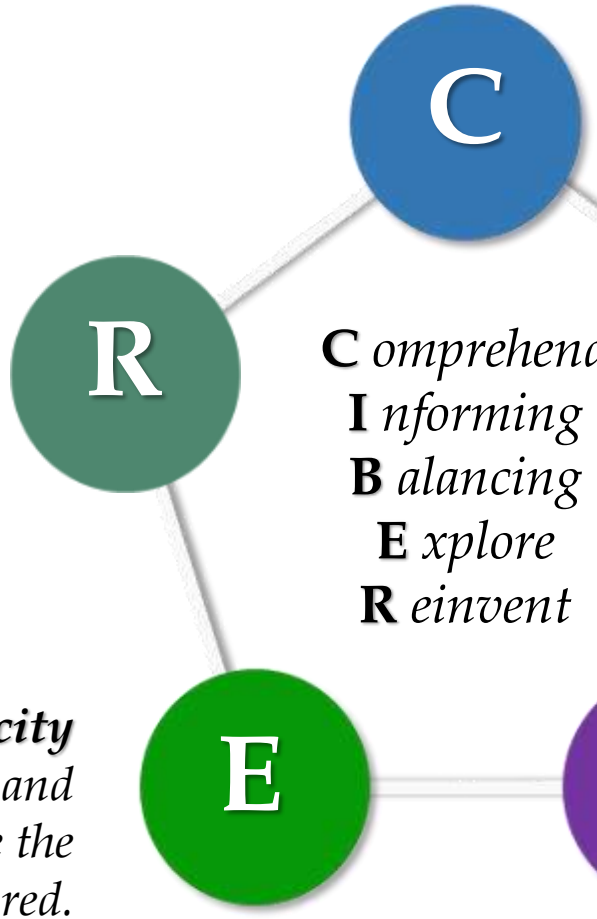
Digital context fundamentals

Cybersecurity strategic fundamentals

Cybersecurity organizational & tactical fundamentals

Cybersecurity technical and operational fundamentals

Key Features of the Cybersecurity Professional



Communication
Explain complex challenges in simple terms. Analogies are useful in this exercise.

Training and experience
Have adequate education and experience in the field.

Frameworks
Identify appropriate resources and tools to do the job.

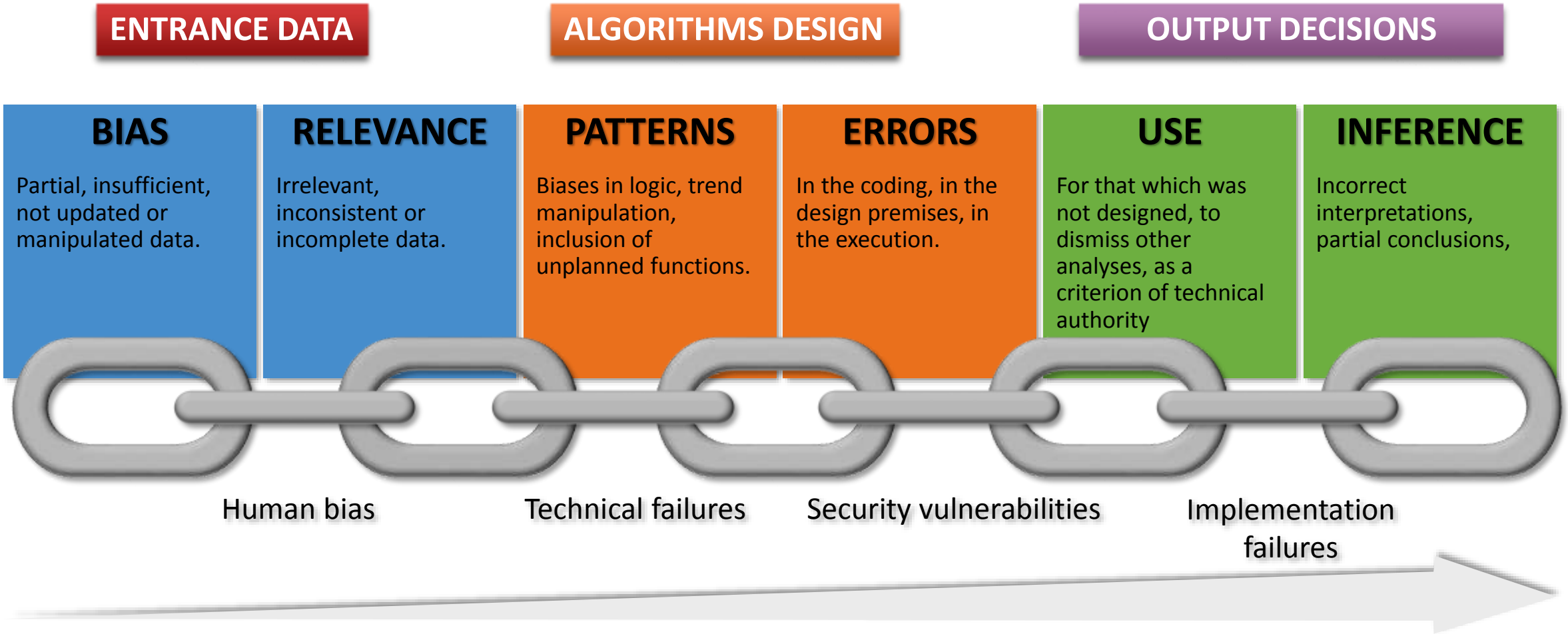
Audacity
Experience uncertainty and doubts and still make the decisions that are required.

Innovation
Accepting mistake as a discovery and an opportunity to overcome cognitive blindness.

Based on: Loftus, G. (2017) Indiana Jones's Five leadership Lessons. *Forbes*. Recuperado de: http://bit.ly/2BKj503

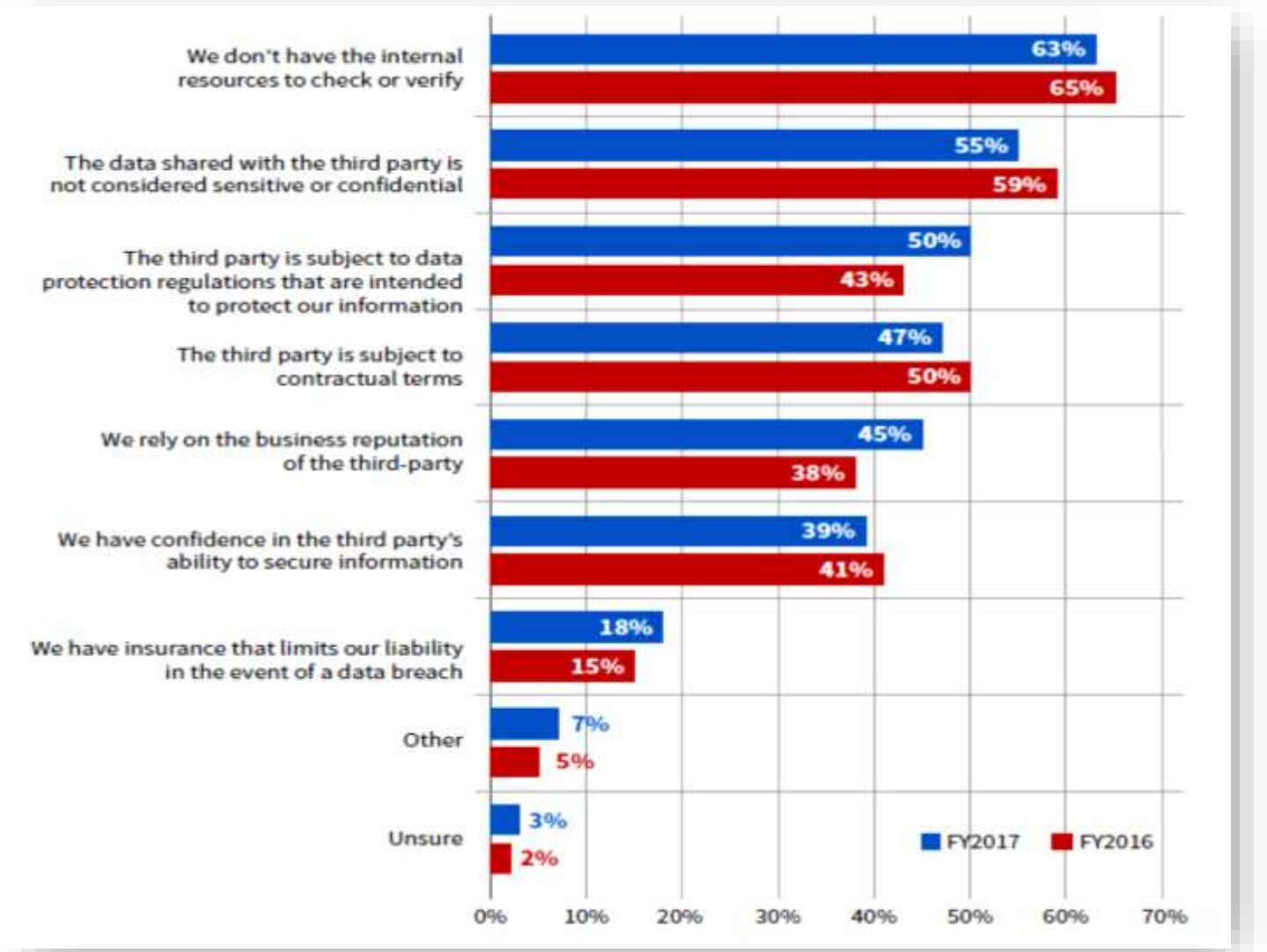
Emergent risks

Artificial Intelligence: Algorithms



Source: Krishna, D., Albinson, N. & Chu, Y. (2017) Managing algorithmic risks. Safeguarding the use of complex algorithms and machine learning. Deloitte. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-algorithmic-machine-learning-risk-management.pdf

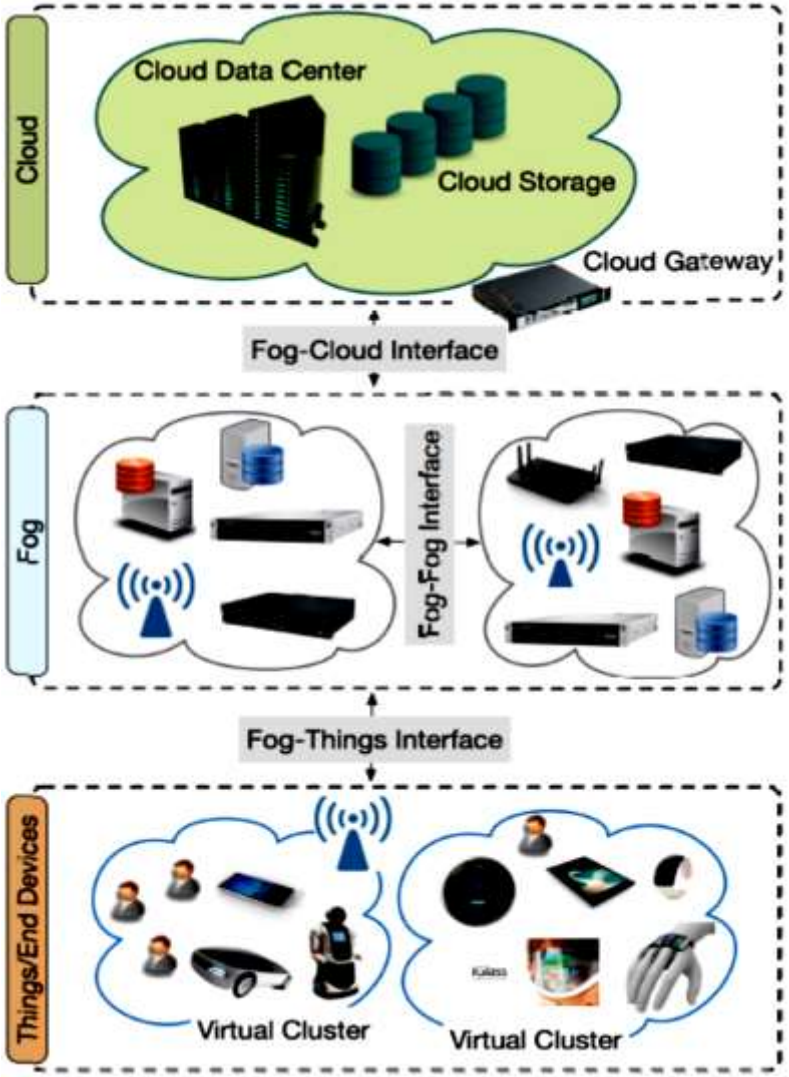
Third Parties: Active monitoring



Source: https://www.opus.com/resource/data-risk-third-party-ecosystem-2nd-annual-study-ponemon-institute/

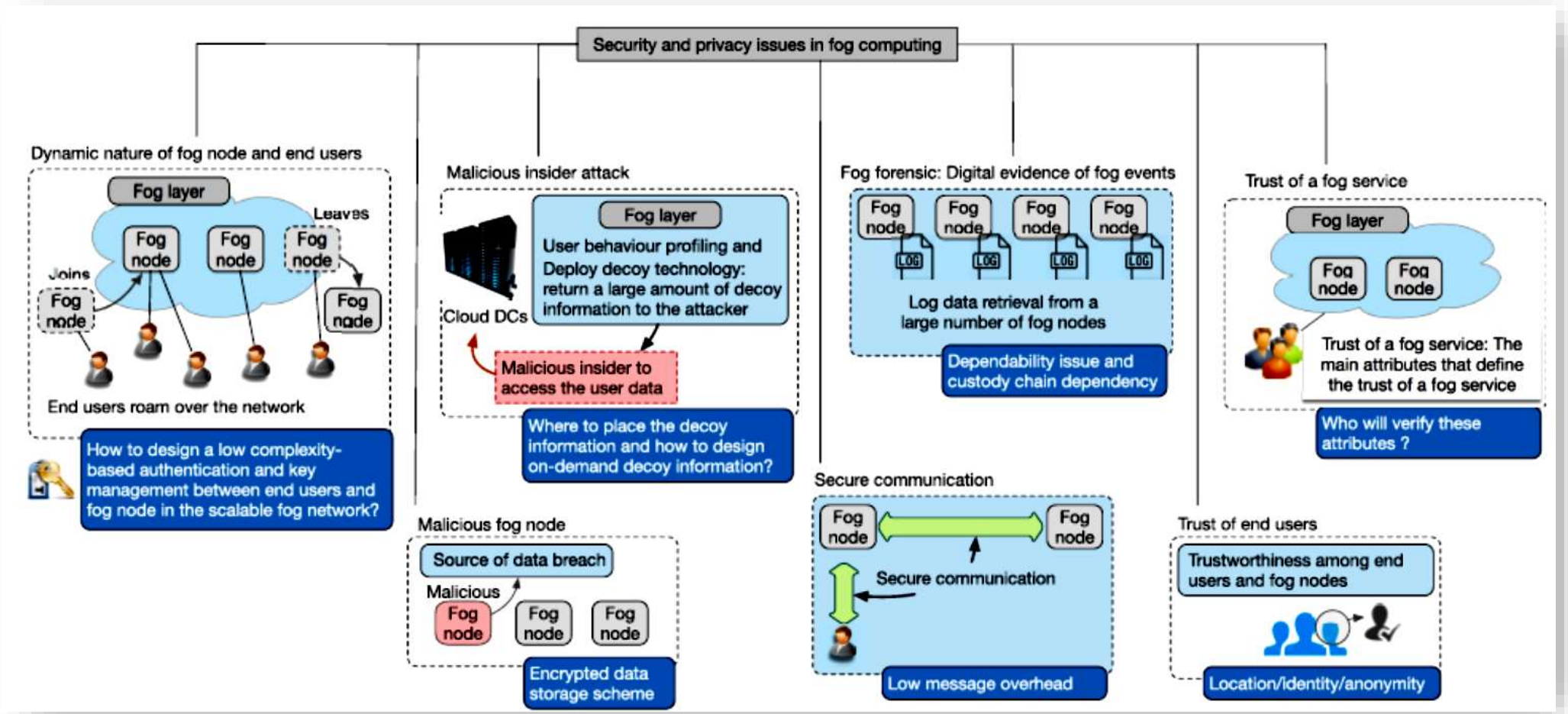
Fog computing: Challenges

Characteristics – *Fog Computing*	Low latency and localization sensitivity.
	Geographic distribution
	Mobility in end device
	Processing capacity in a high number of nodes
	Wireless access
	Real-time applications
	Heterogeneity



Source: Mukherjee, M. et al. (2017) Security and Privacy in Fog Computing. *IEEE Access*. 5. 19293-19304. doi: 10.1109/ACCESS.2017.2749422

Fog computing: Challenges



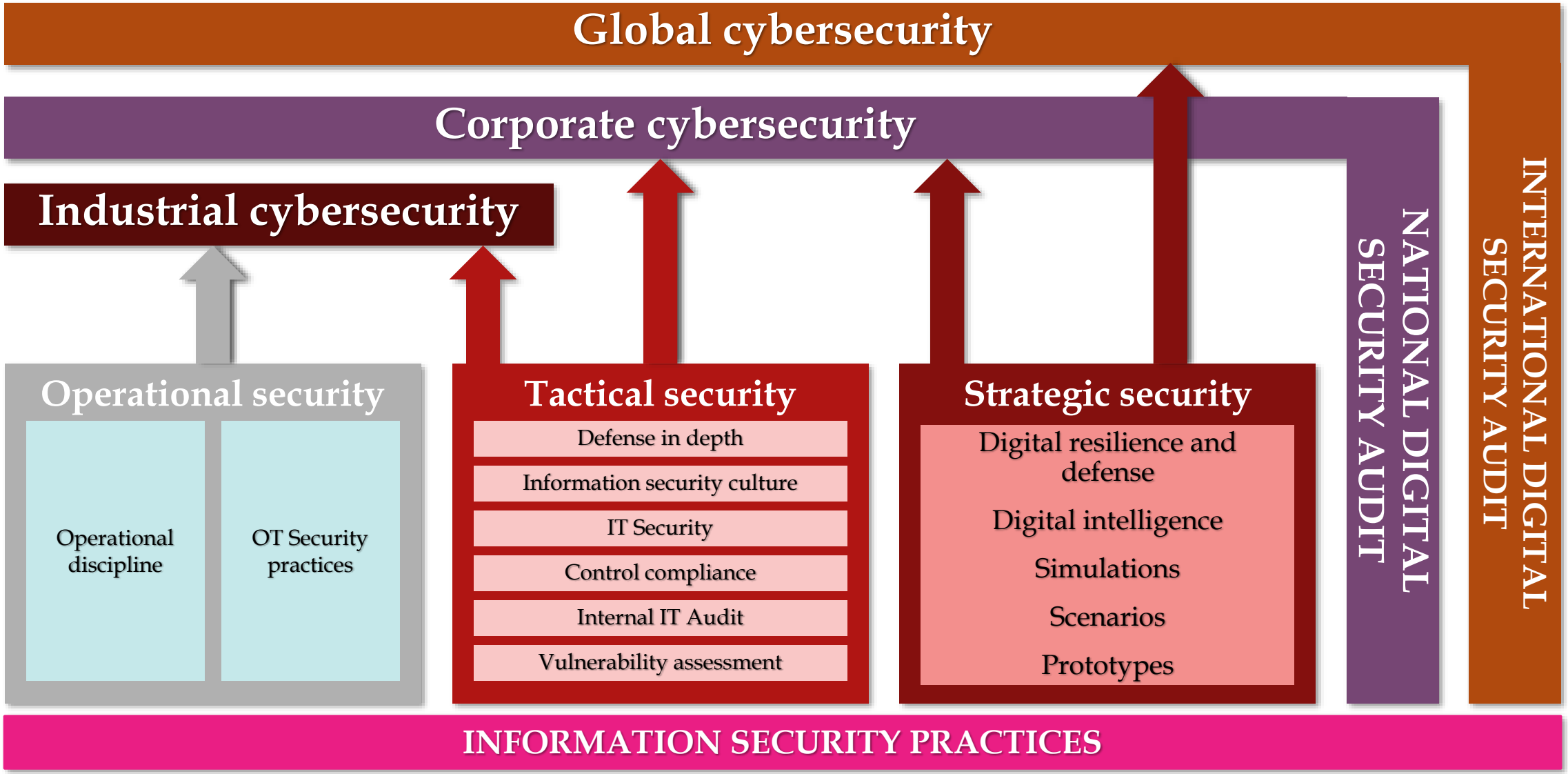
Source: Mukherjee, M. et al. (2017) Security and Privacy in Fog Computing. *IEEE Access*. 5. 19293-19304. doi: 10.1109/ACCESS.2017.2749422

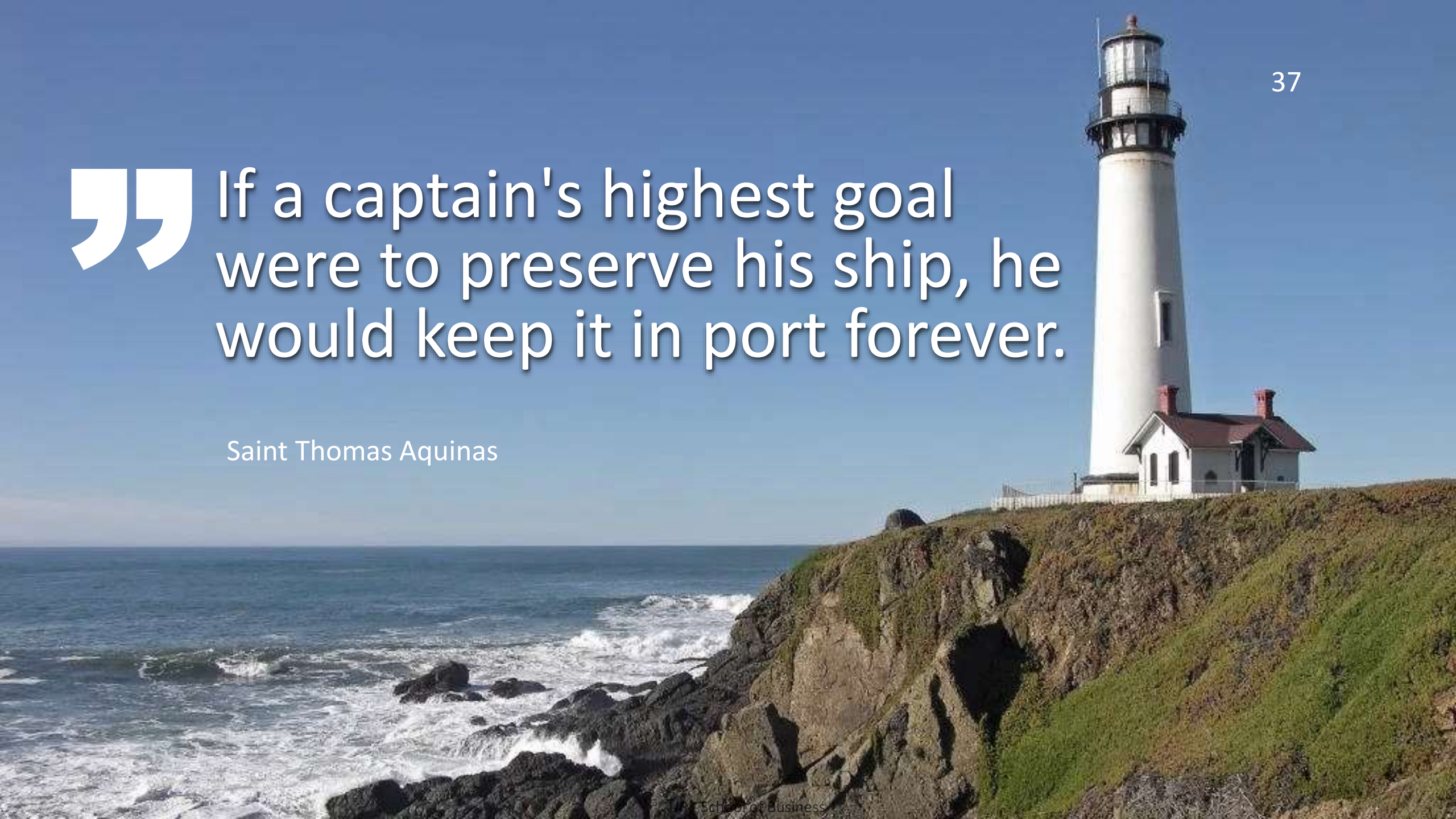
Conclusions

Digital Corporate Responsibility Principles

Principle	*Definition*
***Digital* Administration**	*Ensuring that personal data is handled in accordance with the law and in line with the expectations of those who provide it.*
***Digital* Transparency**	*Demonstrate openness in companies use of personal data*
***Digital* Empowerment**	*Give customers more control over their personal data.*
***Digital* Equity**	*Clarify and potentially increase the benefits that customers receive in return for sharing their data.*
***Digital* Inclusion**	*Using personal data to multiply positive results in society.*

Holistic View of Digital Security




If a captain's highest goal were to preserve his ship, he would keep it in port forever.
Saint Thomas Aquinas


EXIT 1A
CYBERATTACK
NEXT EXIT

Liels Paldies !!

Security and Technologies - Future Cyberskills -

Jeimy J. Cano M., Ph.D, CFE
Associate Professor
Universidad del Rosario
School of Business

@itinsecure

jeimy.cano@urosario.edu.co