Strategic ICT Management. Introduction

Prof. Tatjana Volkova

This course serves as a basis

- to provide a theoretical background for establishing the necessary ***harmony*** between ICT management and the strategic development of the company

«*There are two kinds of companies. Those that have been hacked, and those that have been hacked but don't know it yet"*

House Intelligence Committee Chairman Mike Rogers

Learning outcomes of the course

1

Knowledge and understanding students will know and understand the strategic approach to ICT management

2

Skills: students will gain skills to be able to apply appropriate methods, for alignment of Information security activities with the strategic goals and generic business strategies

3

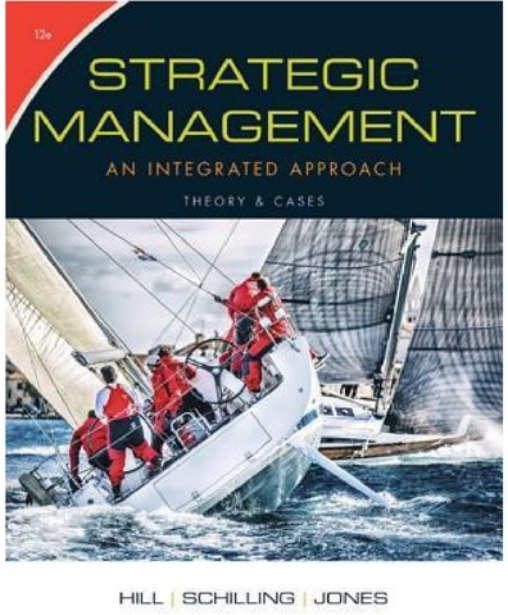
Students will be able to analyze and evaluate strategic management processes to conduct their impact analysis on strategic ICT management

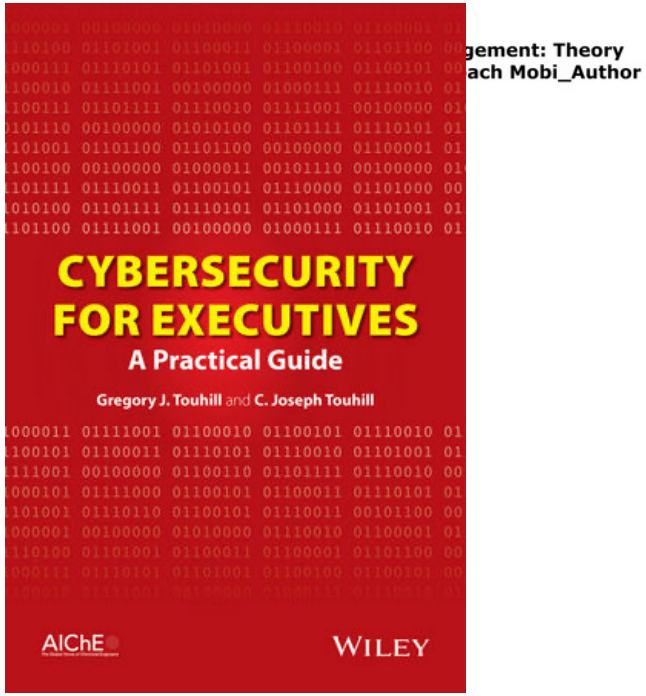
Study course content

- Strategic management process.
- Company strategic directions, internal and external environment analysis. Industry life cycle analysis. CS capabilities.
- Functional, business and corporate level strategies.
- Strategies for competing internationally.
- A strategic approach to ICT governance.
- Information security alignment with strategic directions of development and business processes.

Literature

- Gregory J. Touhill, C. Joseph Touhill Cybersecurity for Executives. A Practical Guide, Wiley, 2014 (part 4 Build your Strategy, p. 95 - 125); https://www.wiley.com/en-us/Cybersecurity+for+Executives%3A+A+Practical+Guide-p-9781118888148
- Hill/Schilling/Jone Strategic Management: Theory an Integrated Approach, 12th Edition, 2017, South–Western Cengage Learning;
- Aligning IT with Business strategy. Guidelines for IT Managers
- Advancing Cyber Resilience Principles and Tools for Boards, WEF, 2017





What is cybersecurity?

What is cybersecurity?

- Very wide term with no standard definition
- Relatively new discipline
- Some believe that CS is something you can buy as a commodity
- Some believe CS refers only to technical measures
- Others believe it is an administrative and technical program
- State of being protected against the criminal or unauthorized use of electronic data, or the measures are taken to achieve this
- What CS means for you?

Do you agree?

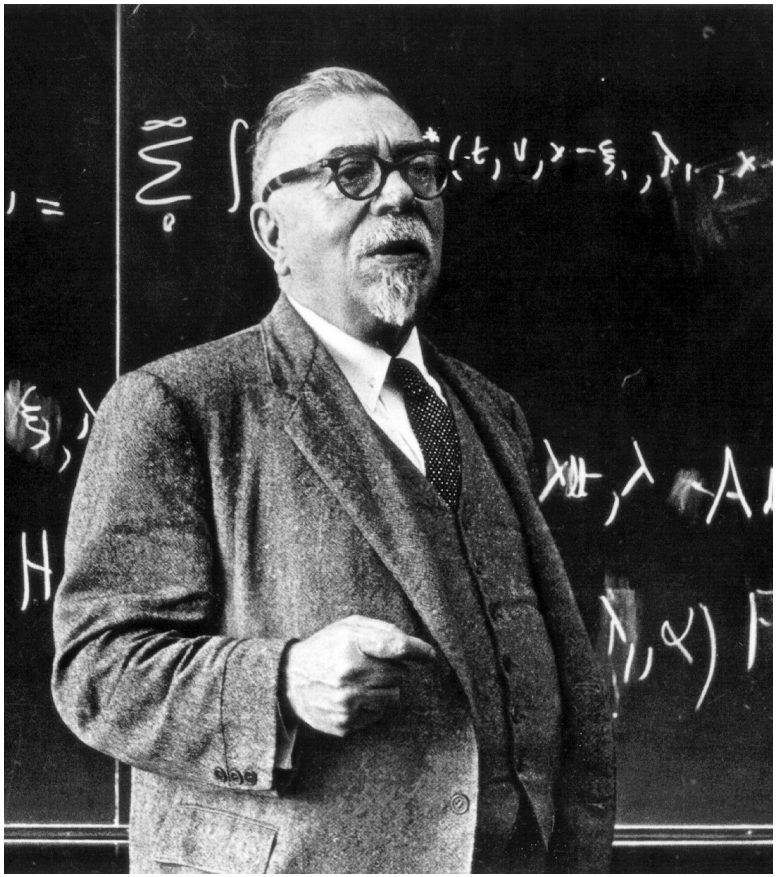
- Cybersecurity is the practice of deploying people, policies, processes and technologies to protect organizations, their critical systems and sensitive information from digital attacks.

The history of 'cyber'

- Cyber is perceived to be a pretty new word, and is often accused of being a word which means nothing. In fact, it actually has quite a long heritage:

- In Ancient Greece, the term *kubernao* was used to mean "steer a ship"
- The Latin *kubernetes* (**steersman or governor)** gives us "cybernetes"
- The Romans turned *kubernao* into *guberno,* from which we get "govern"
- Plato used "*kubernetika*" to mean 'skill in steering'

The history of 'cyber'

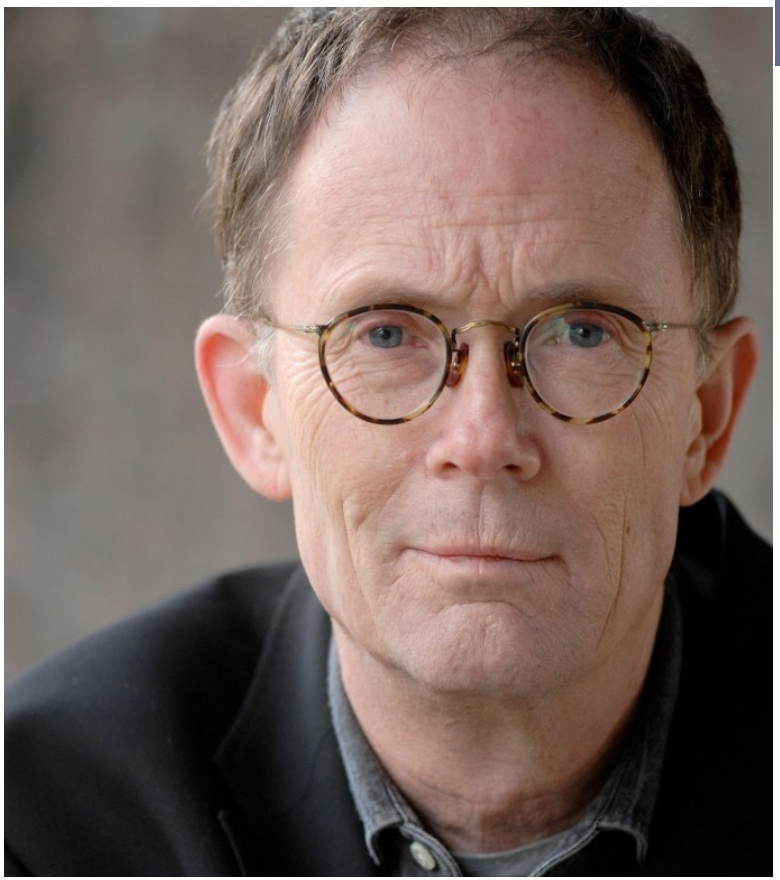


Norbert Wiener (1894 – 1964)

- In the 1940s the American mathematician Norbert Wiener used "cybernetics" to mean "control or regulation mechanisms in human and machine systems",

The history of ‘cyber’

- William Gibson coined the phrase ‘cyberspace’ in his short story Burning Chrome (1982);
- Gibson coined the term "cyberspace" for "widespread, interconnected digital technology”; "mass consensual hallucination" in computer networks.”
- One line from the story—"...the street finds its own uses for things"—has become a widely quoted aphorism for describing the sometimes unexpected uses to which users can put technologies
- Later popularized the concept in his acclaimed debut novel *Neuromancer* (1984).



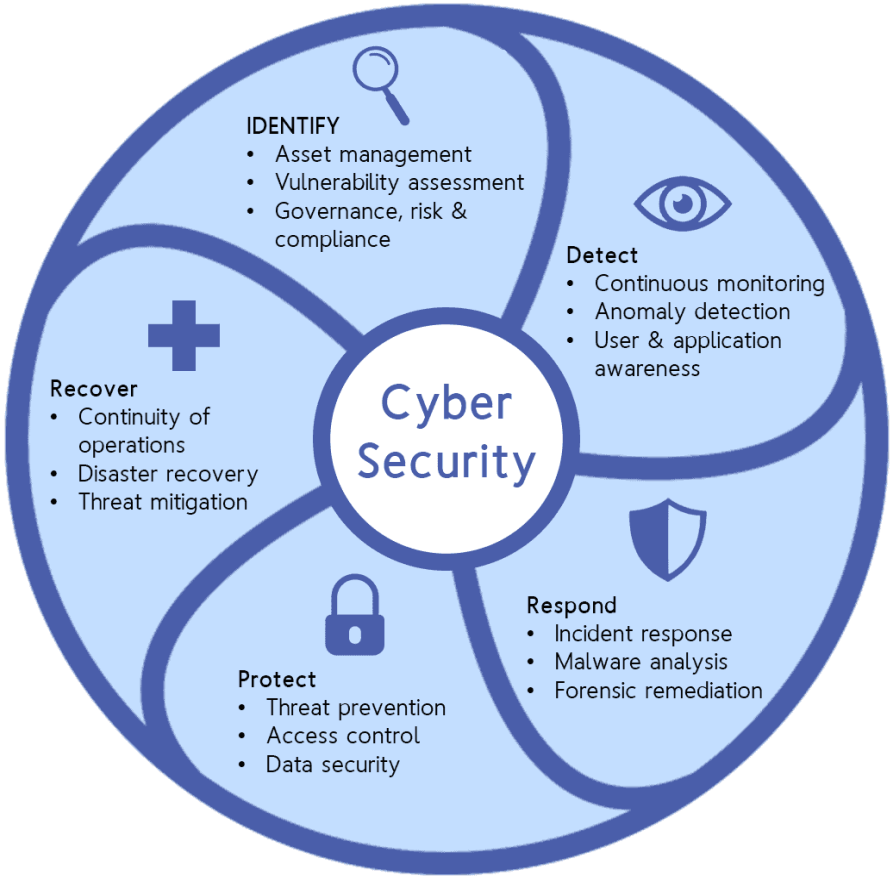
Cybersecurity

- A holistic set of activities that are focused on protecting an organization vital information
- Includes: processes used to create, manage, share and store information
- Includes: practices such as HR training, and testing to ensure information is properly protected and managed
- Effective CS preserves confidentiality, integrity, availability of information, protection from attack by any bad actors, damage of any kind and unauthorized access

Discussion:

- "….We propose that the best way to address cybersecurity is to do so from the perspective of a manager rather than a technologist.
- Cybersecurity is not solely a technical issue. It affects every business function. Every activity in virtually every business relies on information to maintain a competitive advantage.
- Managers at every level need to understand how investing in cybersecurity produces effective, efficient, and secure results. That, in turn, produces value".

Source: *Cybersecurity for Executives: A Practical Guide*, First Edition. Gregory J. Touhill and C. Joseph Touhill. © 2014 The American Institute of Chemical Engineers, Inc. Published 2014 by John Wiley & Sons, Inc.



Group work:

Please identify at least 5 reasons Why CS is so hard? Also from your own experience!

Please share your findings in class!

Time: 15 min

Disucssion:

" As senior executives ourselves, we recognize that a discussion of cybersecurity with fellow executives should not be too "technical,"

- Executives run the entire organization, and they don't need to be focused on the coding techniques of their computer programmers. Rather, their job is to optimize the human and physical resources and assets of the organization in order to fulfil its mission safely, profitably, and beneficially. We understand that a prime focus of executives is risk management, and that is where discussions of cybersecurity should begin.

- *Cybersecurity is about risk management*. It is about protecting your business, your shareholders' investments, and yourself while maintaining competitive advantage and protecting assets. It is not just about IT.

Cybersecurity Management

"While a commonly accepted framework for cybersecurity has not been established, there are some guiding principles, precautions, and technologies that many organizations have chosen to adopt, including:

National Institute of Standards and Technology (NIST) program

Open Web Application Security Project (OWASP) Top 10

International Organization for Standardization (ISO) 27000 series"

Cybersecurity issues

No longer limited to the IT department

Threaten every aspect of the organization

Pose a significant threat to ongoing business continuity and reputation

Extend well beyond the technical environment and reach across the entire business ecosystem

= Cybersecurity solutions must encompass not only technical fixes, but also changes in business processes, controls, management and employee behaviour.

What is a Cyberresilience

- It is the outcome of ability of an enterprise to anticipate, withstand, recover from and evolve to improve capabilities verse conditions, stresses or attacks on the supporting resources it needs to function (National Association of Corporate Directors)
- A holistic approach to understanding and prioritizing business risk and implementing risk management activities need to be integrated in day-to-day activities across all business functions

The cyber quadrant

Figure 1. Four levels of cyber resilience

https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf#zoom=40

ICT management: traditional view

- The goal of ICT infrastructure **management** is to use proven, repeatable processes to provide a stable operating environment for everyone using the technology
- **ICT management** is the management discipline whereby all of the ICT resources of a firm are managed in accordance with its needs and priorities.
- These resources may include tangible investments like computer hardware, software, data, networks and data centre facilities, as well as the staff who are hired to maintain them.

Technology centric VS Business oriented strategies

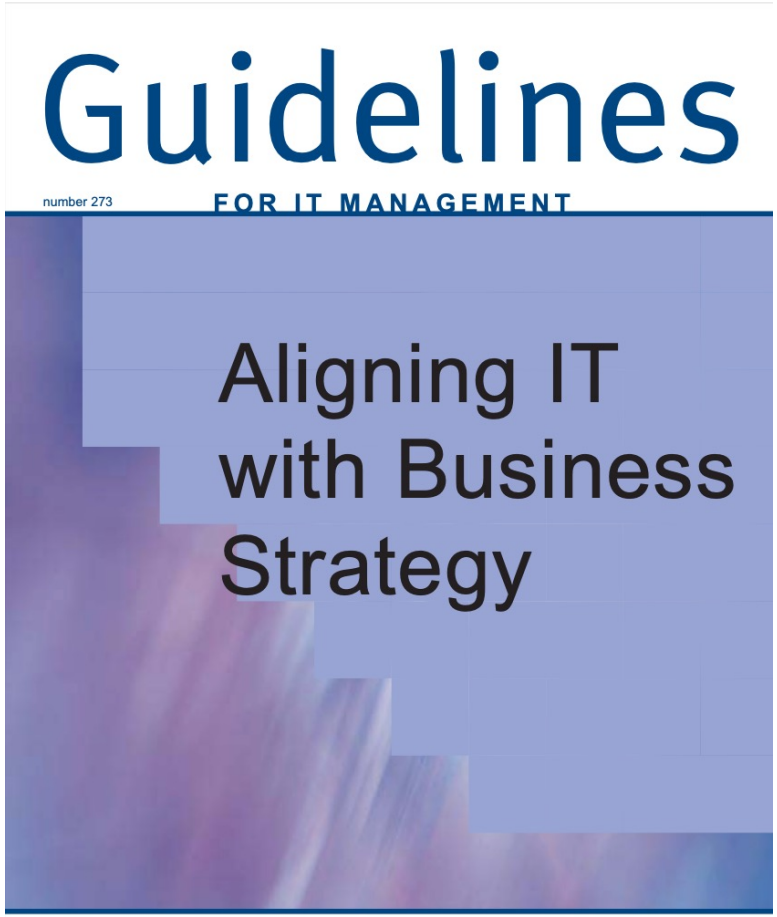
- Alignment of ICT and business strategies is a key issue
- Strategic divergence is counter-productive; leading to complex IT structures that struggle to sustain overlying business operations

Strategic ICT Management

The changing role of ICT:

- IT traditionally been considered as a tool of implementation of strategies, not involved in the company's strategic development
- Due to the changes of business context (VUCA world) , it becomes clear that ICT management has to provide a proactive role in ensuring viable business

Task: please read the text Understanding the Importance of Aligning IT Strategy with Business Strategy and prepare PPP for the next class



number 273 **KEY POINTS**

- The first principle of aligning IT with the business, is a crystal clear understanding of the business itself.
- The most frequently overlooked aspect of IT strategy definition is the cultural analysis of the organisation.
- Understanding value chains is paramount because these represent the relationships and the touch-points between the business functions and the IT estate.
- We need to know what pressures will shape and influence our business; perhaps imposing change upon us when we least welcome it.
- Gather intelligence from a number of sources, both internal and external to determine how any change may affect existing business functions, culture, IT estate and value chains.
- Successfully balancing sometime disparate needs is at the core of IT and Business Strategy alignment.
- Where necessary adjust schedules to accommodate proper alignment with established resource cycles.
- Business units need to move at different speeds – so each business unit should have its own, dedicated, IT programme of work, showing when, where and why activity will be taking place.
- The golden rule is never to over-commit beyond actual capacity to deliver. If there are insufficient resources, or time available within the capacity horizon, either the task must be re-formulated, or the resource pattern altered.
- Continually review all work in progress to see if current plans have been impacted unexpectedly by changing circumstances – vigilance is just as important as vision.
- The essence of successful alignment between IT and the Business Strategy is based on effective understanding, communication, collaboration and mutual trust.

The National Computing Centre Limited,
Oxford Road, Manchester M1 7ED, United Kingdom.
Tel: +44 (0)161-242 2121 Fax: +44 (0)161-242 2499
http://www.ncc.co.uk e-mail:info@ncc.co.uk

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Future of Digital Economy and Society System Initiative

Advancing Cyber Resilience
Principles and Tools for Boards

In collaboration with The Boston Consulting Group and Hewlett Packard Enterprise

January 2017

Contents

3. Cyber Resilience Principles and Tools for Boards

3.1 Board Principles for Cyber Resilience

Principle 1

Responsibility for cyber resilience. The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. risk committee) or new committee (e.g. cyber resilience committee).

Principle 2

Command of the subject. Board members receive cyber resilience orientation upon joining the board and are regularly updated on recent threats and trends – with advice and assistance from independent external experts being available as requested.

Principle 3

Accountable officer. The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

Principle 4

Integration of cyber resilience. The board ensures that management integrates cyber resilience and cyber risk assessment into overall business strategy and into enterprise-wide risk management, as well as budgeting and resource allocation.

Principle 5

Risk appetite. The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Principle 6

Risk assessment and reporting. The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber Risk Framework.

Principle 7

Resilience plans. The board ensures that management supports the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

Principle 8

Community. The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.

Principle 9

Review. The board ensures that a formal, independent cyber resilience review of the organization is carried out annually.

Principle 10

Effectiveness. The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

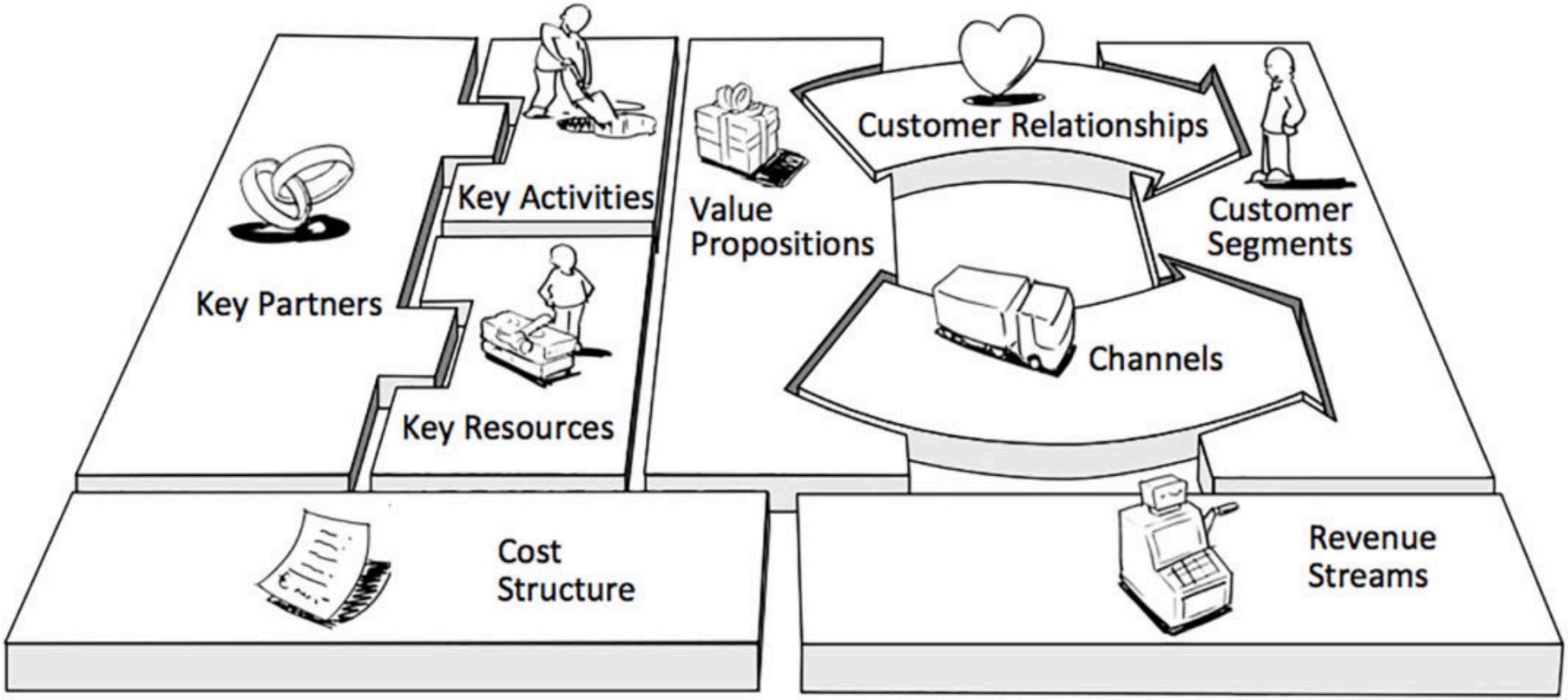
Individual task: please provide the critical feedback on the Board principles for CR

ICT alignment with business

The role of ICT function is capturing, processing, storing, distribution information or data;

The first principle of aligning ICT with business – *understanding business itself to achieve desired outcomes;*

There is necessary to integrate ICT activities within business **overall business model** to ensure the competitiveness of business



Defining an Industry

- Industry
  - A group of companies offering products (goods or services) that are close substitutes for each other and satisfying the same needs of clients;
- Competitors
  - Companies that serve the same basic customer needs
- Sector
  - A group of closely related *industries*
- Market segments
  - Distinct groups of customers within a market that can be differentiated from each other based on their distinct attributes and demands
- Changing industry boundaries

http://www.census.gov/eos/www/naics/index.html

You are here: Census.gov › Business & Industry › NAICS

North American Industry Classification System

Main | History | Development Partners | Federal Register Notices | NAPCS | FAQs

NAICS Search:

Enter keyword or 2-6 digit code

2012 NAICS Search

Enter keyword or 2-6 digit code

2007 NAICS Search

Enter keyword or 2-6 digit code

2002 NAICS Search

Downloads/Reference Files/Tools

- 2012 NAICS

Introduction to NAICS

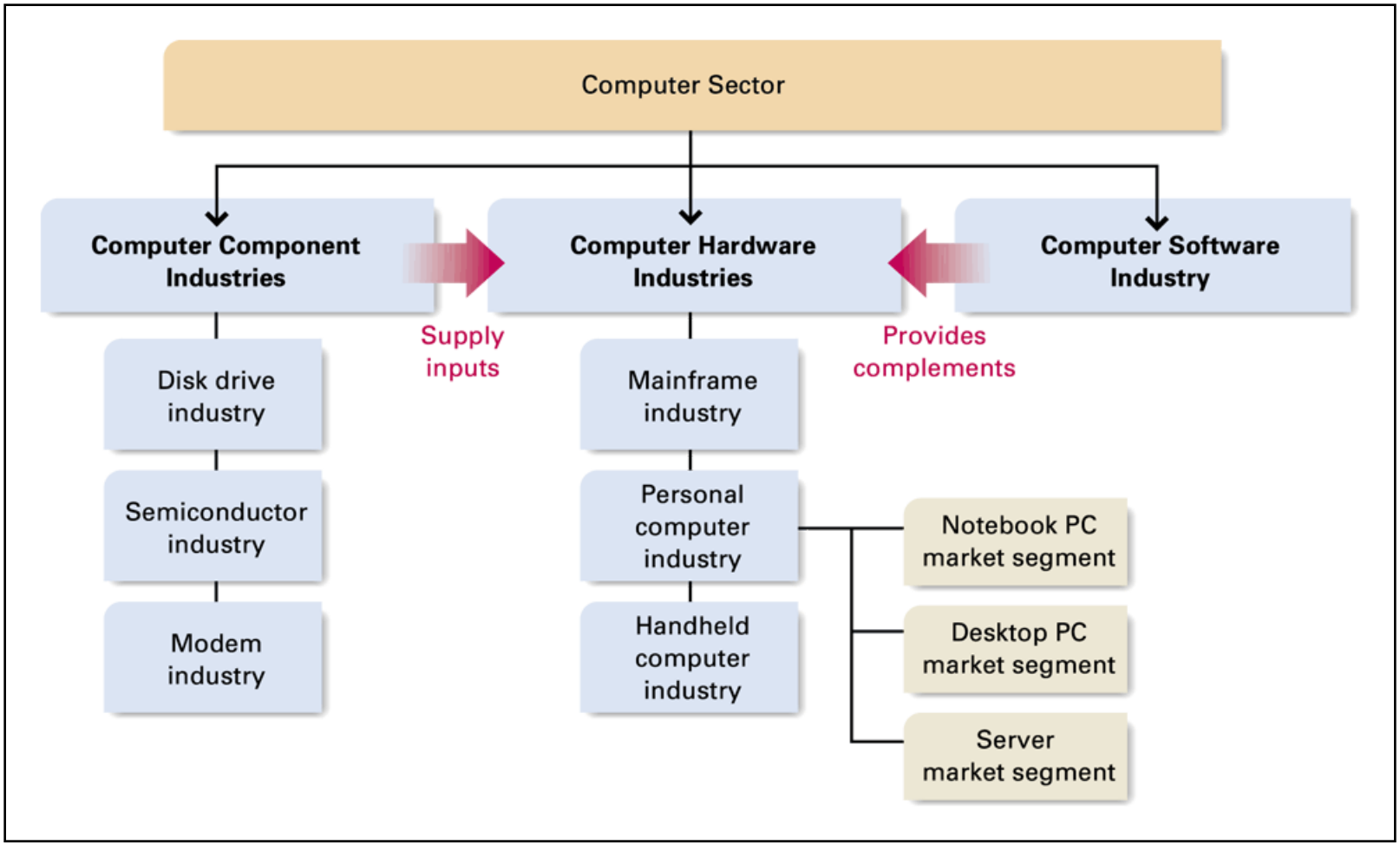
The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy.

NAICS was developed under the auspices of the Office of Management and Budget (OMB), and adopted in 1997 to replace the Standard Industrial Classification (SIC) system. It was developed jointly by the U.S. Economic Classification Policy Committee (ECPC), Statistics Canada, and Mexico's Instituto Nacional de Estadistica y Geografia, to allow for a high level of comparability in business statistics among the North American countries.

This official U.S. Government Web site provides the latest information on plans for NAICS revisions, as well as access to various NAICS reference files and tools.

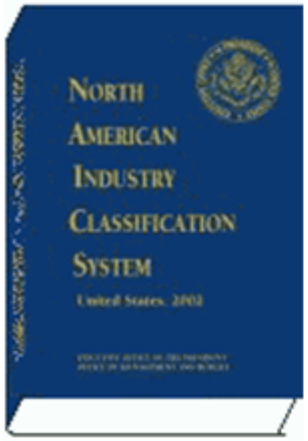
The official 2012 U.S. NAICS Manual includes definitions for each industry, background information, tables showing changes between 2007 and 2012, and a comprehensive index. The official 2012 U.S. NAICS Manual is available in print and on CD-ROM from the National Technical Information Service (NTIS) at (800) 553-6847 or (703) 605-6000, or through the NTIS Web site. Previous versions of the NAICS Manual are available.

The Computer Sector: Industries and Segments



North American Industry Classification System (NAICS)

This is the official U.S. Government site to order either the printed or CD-ROM version of the NAICS Manual



Technical Report

◉ **$62.00**-2012 Edition (Hardback)

Order No. **PB2012100001** (Price outside the U.S., Canada and Mexico $124)

○ **$79.00**-**2012 CD-ROM with search and retrieval software**. (Price outside the U.S., Canada and Mexico $159)

Order No. **PB2012-500003**

The CD-ROM requires Adobe Acrobat Reader.

Add to Cart

To Order:

- Call NTIS a **1-800-553-6847** or **(703) 605-6000**
- Most major credit cards accepted.
- Fax your **order form** to **(703) 605-6900.**

A product of Office of Management and Budget's Economic Classification Policy Committee

NAICS will reshape the way we view our changing economy

Department of Commerce, Bureau of Census

The *North American Industry Classification System (NAICS)* has officially replaced the U.S. Standard Industrial Classification (SIC) system. The NAICS provides a consistent system for economic analysis across the three North American Free Trade Agreement partners Canada, Mexico and the United States.

STRA

North American Industry Classification System (NAICS) Canada 2017 Version 3.0

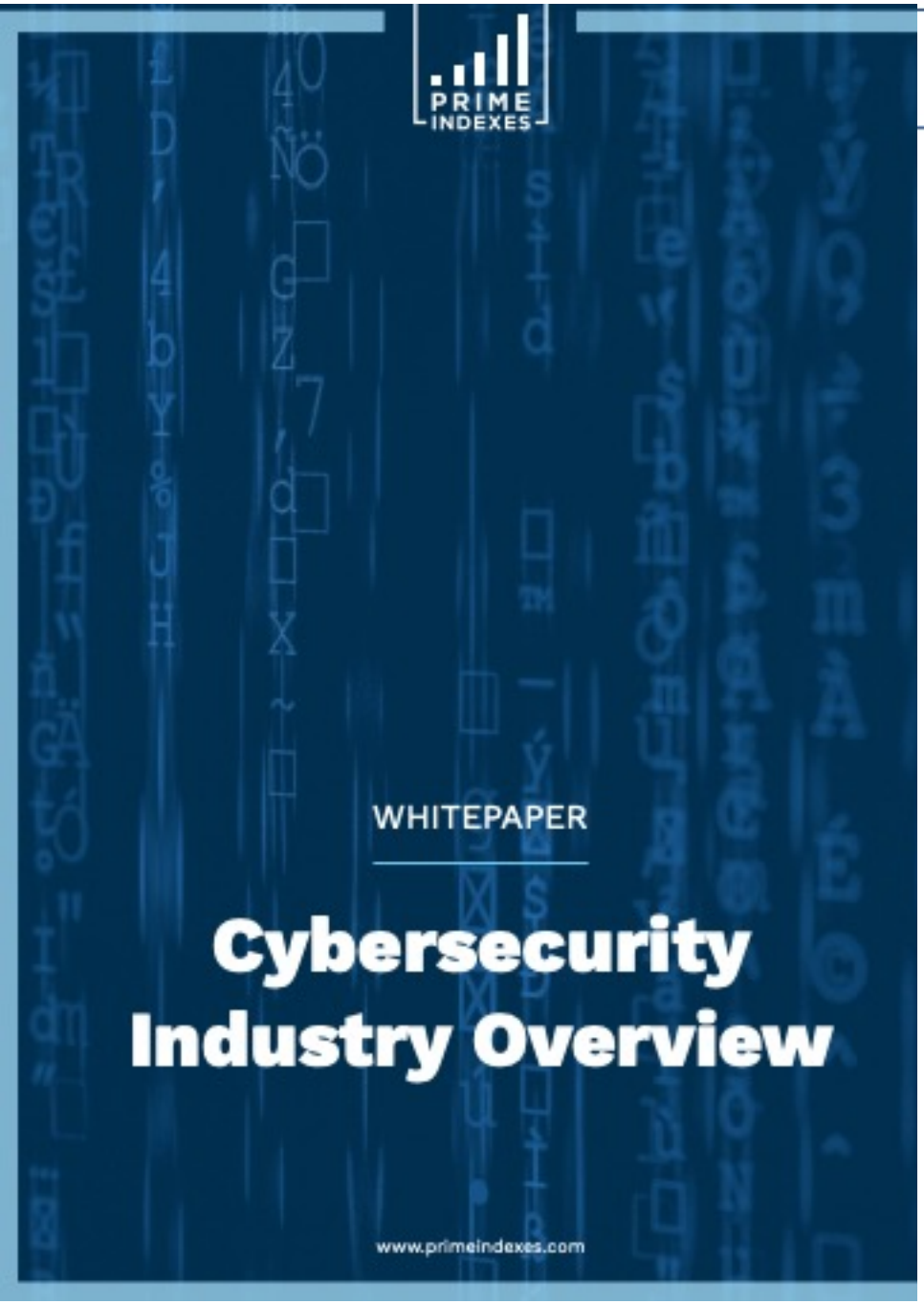
Participate in the revision of the North American Industry Classification System (NAICS) Canada
Updated on: December 20, 2019

Status

This standard was approved as a departmental standard on October 16, 2017.

NAICS 2017 version 3.0

The North American Industry Classification System (NAICS) has been developed by the statistical agencies of Canada, Mexico and the United States. However, Statistics Canada has created 5 cannabis industries that are unique to NAICS Canada 2017 Version 3.0.



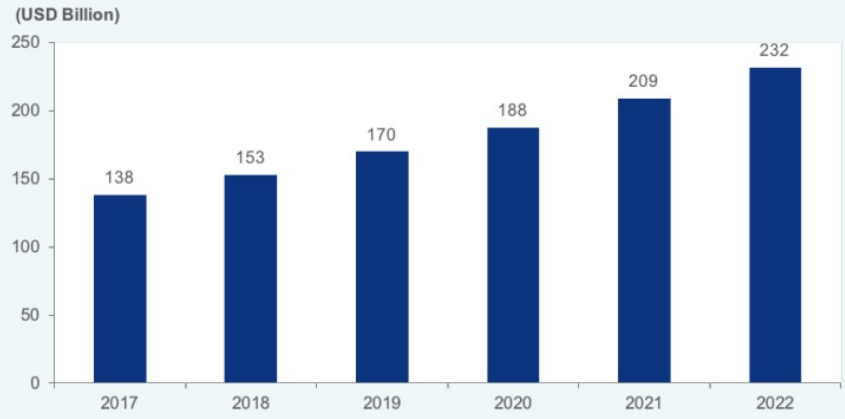
Contents

https://etfmg.com/wp-content/uploads/2019/03/26-Prime-Indexes-CyberSecurity-Industry-Review-14112019.pdf

Cybersecurity: Industry Trends and Future Prospects

The global cybersecurity market grew from $3.5 billion in 2004 to about $138 billion in 2017 –over 39x in 13 years. In 2017, the aerospace and defense vertical had the largest share in the cybersecurity market. However, going ahead, government, BFSI and IT and telecom verticals are expected to gain traction. During 2017 to 2022, the cybersecurity market is expected to grow at a CAGR of 11% to reach $231.94 billion. North America dominated the global cybersecurity market in 2017, this trend is also expected to change as APAC is estimated to grow at the fastest pace during 2017-2022.[79,80,81]

Size of the Cybersecurity Market Worldwide



Source: Statista,2018[82]

Rise of IoT will require more sophisticated security solutions: The use of big data, autonomous vehicles, virtual assistants, cloud computing, and IoT/connected devices will increase our susceptibility to cyberattacks. However, cybersecurity will also evolve rapidly and create robust self-healing and self-defending networks by leveraging AI and blockchain. AI-based security solutions will increasingly be deployed by organizations to shore up defense and protect valuable data. Alphabet Inc. has already provided a promising solution. Chronicle, a security company (Alphabet's subsidiary) that uses AI-based solutions for the cybersecurity industry, claims to deploy planet-scale computing and analytics to fight cybercrime on a global scale.[83,84,85,86,87,88]

Cybercrime will evolve as a business: Cybercriminals will increasingly use more computing power and complex techniques, and threats such as phishing, mobile malware and ransomware will evolve and become more sophisticated. Amateur hackers are already changing their modus operandi, making it a professionally run business. Sophisticated attacks on critical infrastructure and supply chain will increase. This would give a big boost to the ethical hacking industry, which, in turn, would bolster the cyber security industry.[89,90]

Companies have a great expectations from investments in ICT for future benefits to the business:

- reduce costs
- improve productivity
- deliver innovations
- improve efficiency
- improve quality
- improve risk management
- implement new business strategies

- gain competitive advantage by exploiting new ICT
- etc.

In order to align ICT with overall business ‘strategies have to be

- formulated
- visible;
- well communicated;
- well understood;
- supporting fulfillment of business mission and goals;

Incorporating cybersecurity into business strategic development

Strategic development team must consider cybersecurity as an essential part of their thought process

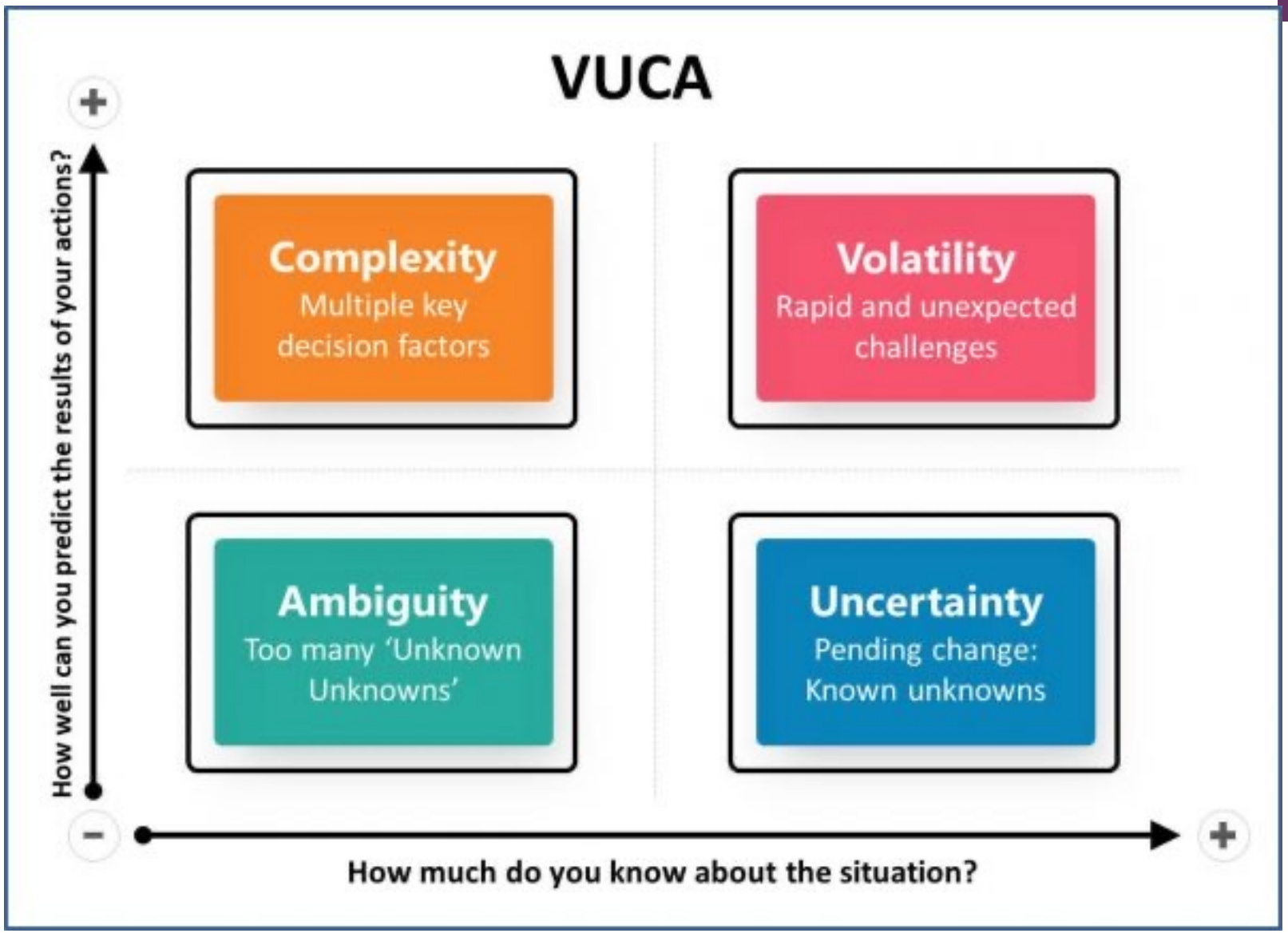
Strategic development team has to include ICT expert to help to guide strategic development development from a cybersecurity perspective

Divergent thinking is applied as a **thought** process or method used to generate creative ideas by exploring many possible solutions. It typically occurs in a free-flowing, "non-linear" manner, such that many ideas are generated in an emergent cognitive fashion;

What would you answer to the Q:
How much do I need to invest in cybersecurity?

It depends on company

- SIZE
- INDUSTRY & BUSINESS MODEL
- GROWTH AGENDA
- INTERNATIONAL PRESENCE
- GENERIC STRATEGIES
- LEVEL OF CS AWARENESS, ETC.


VUCA
Complexity
Multiple key decision factors
Volatility
Rapid and unexpected challenges
Ambiguity
Too many 'Unknown Unknowns'
Uncertainty
Pending change: Known unknowns
How well can you predict the results of your actions?
How much do you know about the situation?

Course requirements: final individual work

- Conduct an interview of ICT manager of chosen company regarding the strategic approach to ICT management and the main issues related its application;
- The critical analysis of findings has to be given in a Report form;