PROMOTING EFFECTIVE CYBERSECURITY MANAGEMENT IN DEVELOPING ECONOMIES: THE CYBERSECURITY CAPABILITY MATURITY MODEL

Corlane Barclay

University of Technology Jamaica

ITU-D Study Group 2 Meeting, September 22-26 2014

CYBERSECURITY & DEVELOPING ECONOMIES

- The cost of cybercrime continues to grow
  - Latest Norton Report estimates it at over US$113B.
- Developing economies are at a higher risk of cybercrimes and threats
  - Vulnerable information infrastructure
  - Limited capabilities
  - Limited resources

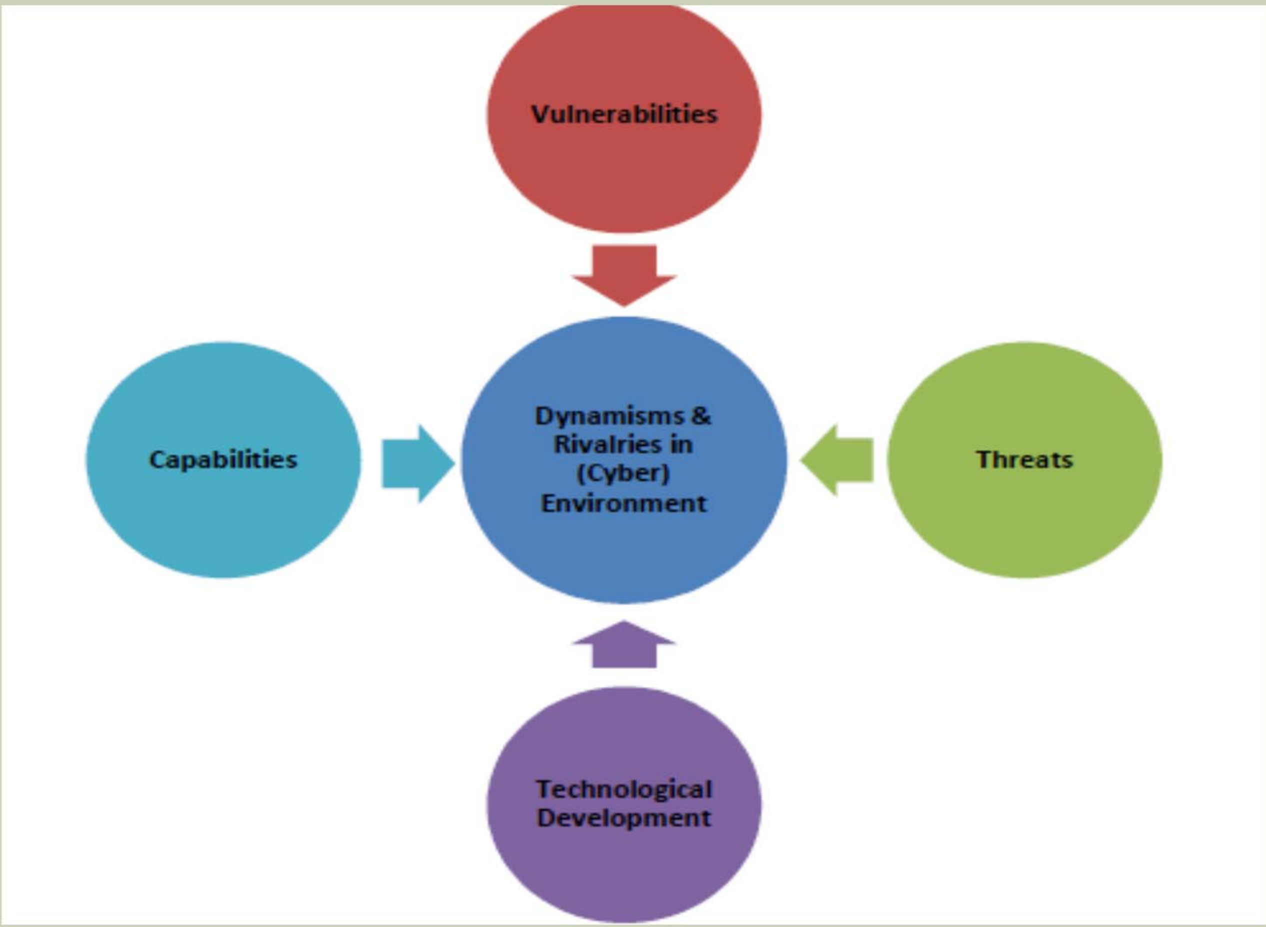
CYBERSECURITY MANAGEMENT

- Cybersecurity is the process of protecting assets (including people) from vulnerabilities, unintended or unauthorized intrusion.
- *“the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.” – ITU*
- The focus on managing cybersecurity should be less on the threats and more on **how one may be threaten** and **what is needed to deter and defend against such threats.**
  - Thereby attaining *security advantage*
- The research therefore introduces two main artifacts -
  - A **5-factor model** to help guide cybersecurity planning and management.
  - A 6-stage **Cybersecurity Capability Maturity Model** that addresses the paradigm shift from threat-based to capability-based management of cybersecurity.

(CYBER)SECURITY ADVANTAGE

- The state of awareness and preparedness to defend against threats in a changing environment.
- The ability to effectively assess, plan, manage, and respond to threats and vulnerabilities through a capability-centric approach.
  - continued analysis of the environment to identify changes and shifts;
  - critically examine how cyber criminals and insiders may act;
  - address any weaknesses and vulnerabilities in the critical information assets and people; and
  - improve the necessary resources and capabilities (know-how) needed to achieve a more secured cyber and information environment

5-FACTOR MODEL OF THE CYBER-ENVIRONMENT


Vulnerabilities
Capabilities
Dynamisms & Rivalries in (Cyber) Environment
Threats
Technological Development

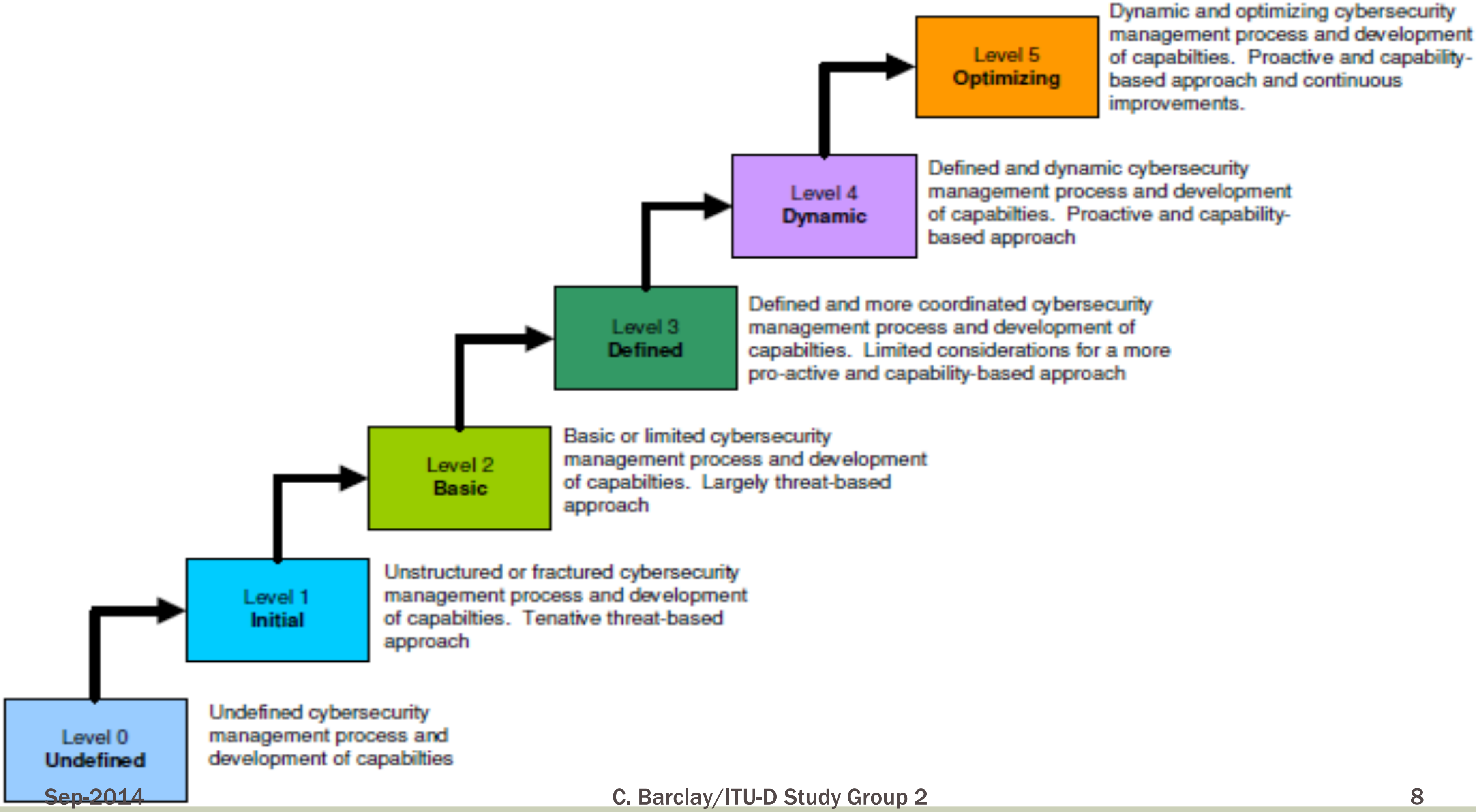
5-FACTOR MODEL

- It is proposed that to achieve sustainable security advantage countries need to dynamically build its capabilities to counter threats, vulnerabilities and advance with technology.
- Dynamisms in environment
  - Any changes in the internal and external that may impact security
- Threats
  - Any potential dangers or risks from both insiders and outsiders
- Vulnerabilities
  - Any form of exposure present or inherent in the information infrastructure and people
- Capabilities
  - Resource capacity in the form of *society, technical, operational, business, legal and regulatory, and education and capability building measures*
- Technological Development
  - Effective use of technology to create innovative artifacts to serve as improved resilence

CYBERSECURITY CAPABILITY MATURITY MODEL

- There are 6 capability and maturity levels for improving security advantage and cybersecurity management
- Level 0. Undefined or Prenatal;
- Level 1. Initial or Infant;
- Level 2. Basic or Child;
- Level 3. Defined or Adolescent;
- Level 4. Dynamic or Adult;
- Level 5. Optimizing or Sage.

CYBERSECURITY CAPABILITY MATURITY MODEL



Level 5
Optimizing

Dynamic and optimizing cybersecurity management process and development of capabilties. Proactive and capability-based approach and continuous improvements.

Level 4
Dynamic

Defined and dynamic cybersecurity management process and development of capabilties. Proactive and capability-based approach

Level 3
Defined

Defined and more coordinated cybersecurity management process and development of capabilties. Limited considerations for a more pro-active and capability-based approach

Level 2
Basic

Basic or limited cybersecurity management process and development of capabilties. Largely threat-based approach

Level 1
Initial

Unstructured or fractured cybersecurity management process and development of capabilties. Tenative threat-based approach

Level 0
Undefined

Undefined cybersecurity management process and development of capabilties

LEVEL 0/UNDEFINED

- Characterized by an undefined process which is the lowest possible level of capabilities.
- Lack of presence in any coordinated response to threats and vulnerabilities
- Undefined process in the development of capabilities
- Undefined process in technological development

LEVEL 1/INITIAL

- Characterized by an initial process that is at an infancy level and efforts are predominantly fractured and disconnected. Generally, only one area of capability is the
- Any response is largely reactive and threat-based.
- Fractured process in the development of capabilities
- Undefined or fractured process in the area of technological development
  - Limited effective use of technology
  - Primarily customers instead of producers

LEVEL 2/BASIC

- Characterized by a basic or limited range of response efforts to cybersecurity.
- Any response is largely reactive and threat-based.
- Limited scope in the process of the development of capabilities
- Limited attention in the area of technological development
  - Limited effective use of technology
  - Primarily customers instead of producers

LEVEL 3/DEFINED

- Characterized by a defined process that improves on the basic stage where the approach is more coordinated, and likely to be government or agency led.
- Presence of a shift to a more proactive stance but still primarily reactive and threat-based.
- Defined process in the development of certain capabilities
- Defined process in the area of technological development
  - Shift to more effective use of technology
  - Balanced mix of customers and producers of technology

LEVEL 4/DYNAMIC

- Characterized by a dynamic process where a capability-centred approach to cybersecurity management is undertaken with strong coordinated and proactive measures.
- A proactive and capability-based response perspective.
- Defined and dynamic process in the development of core capabilities
- Defined and dynamic process in the area of technological development
    - Shift to innovative exploitation of technology
    - Shift to producers of technology

LEVEL 5/OPTIMIZING

- Characterized by an optimizing process where a capability-centred approach to cybersecurity management is undertaken with coordinated proactive measures.
- A proactive and capability-based response perspective.
    - All the pillars of capabilities are harnessed with strong emphasis on innovation and research with advanced prevention and detection measures available across key sectors of society.
- Optimizing process in the development of core capabilities
- Optimizing process in the area of technological development
    - Innovation

CONCLUSION

- Research underlines the importance of achieving and maintaining security advantage in the today's society, particularly at risk or vulnerable economies.
- Identifies some key considerations or areas in the development of cybersecurity management strategies -
  - Awareness of changes in external and internal environment
  - Development of core capabilities
  - Focus on effective and innovative use of technology to response to cybersecurity matters
- Future works involve further development of the security advantage construct and the 5-factor model, development and refinement of the maturity/capability levels, and analysis of countries and organizations that fit at different stages.

CONTACT

- Presentation based on my paper entitled: ***Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model.***
- Proceedings of the ITU Kaleidoscope Academic Conference 2014 and published in IEEE Xplore Digital Library.
- 10.1109/Kaleidoscope.2014.6858466
- Email Contact - *CLBarclay@gmail.com*