CyberSecurity MALAYSIA

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

In conjunction with WIF-KL 2012

WIF KL WORLD INNOVATION FORUM KUALA LUMPUR

csm-ace 2012 CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION

CYBERSECURITY RISK & COMPLIANCE FOR ECONOMIC TRANSFORMATION

www.csm-ace.my

Should Standards be Mandated?

Professor Abu Bakar Munir

University of Malaya

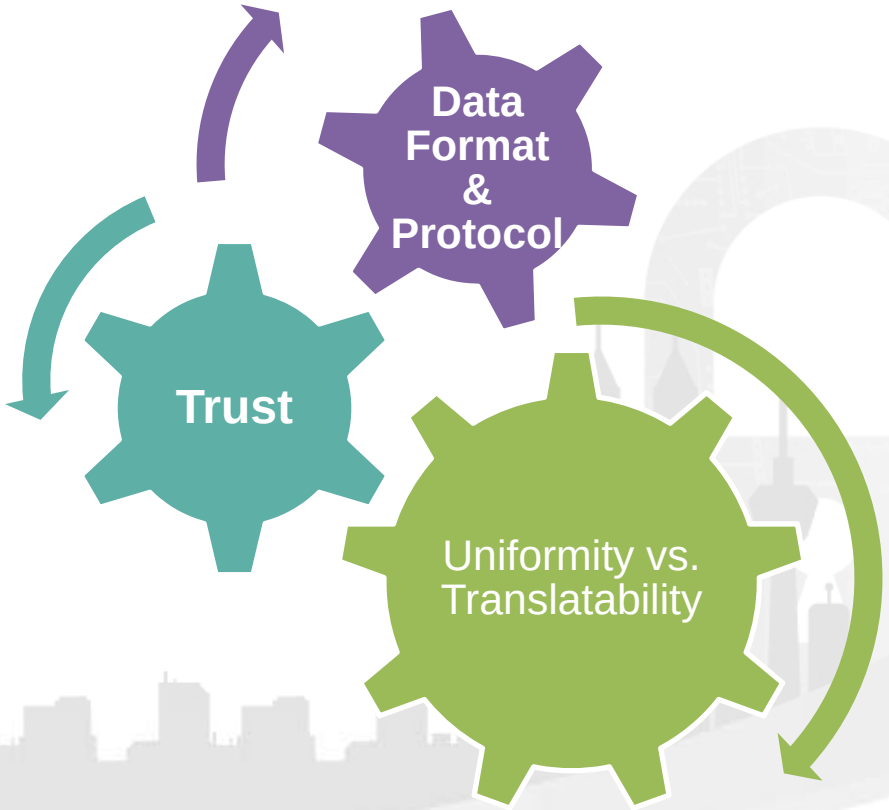
7 November 2012

About cyber security Standards

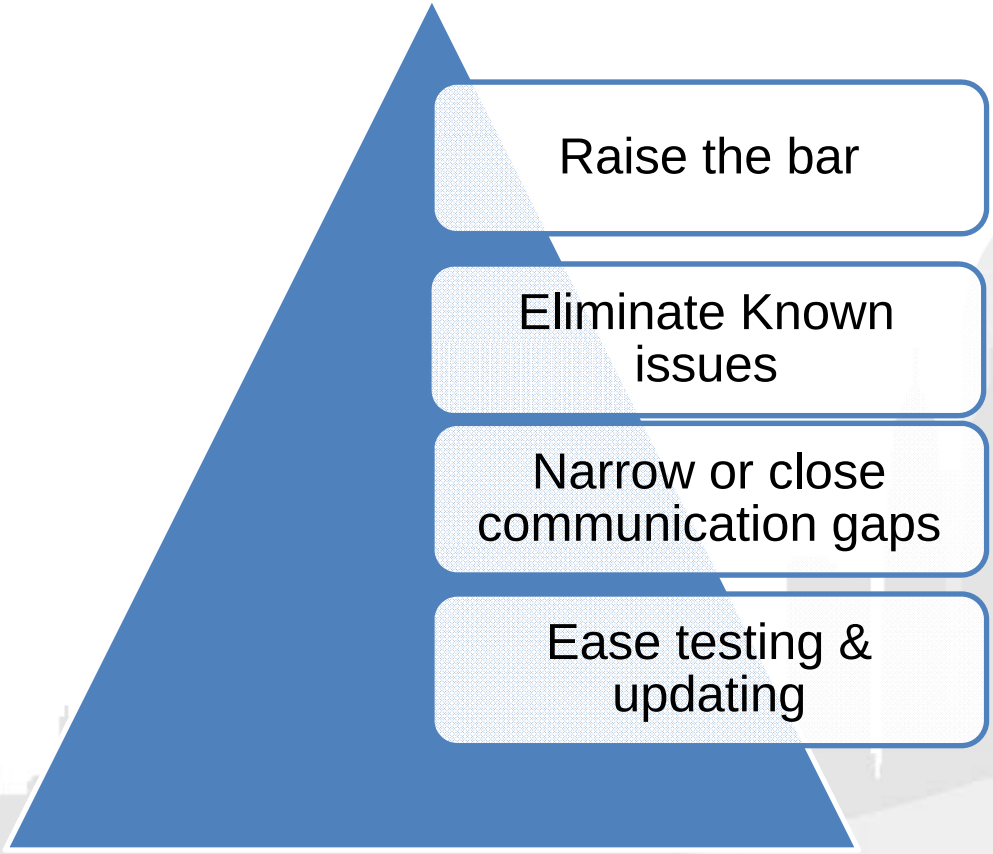
- assist organizations to practice safe security techniques to minimize attacks in Cyber space.
- used as guard against identity theft, trade secrets, proprietary information, and personally identifiable information (PII) of customers or employees

What Standards can do

Interoperability



Baseline


Raise the bar
Eliminate Known issues
Narrow or close communication gaps
Ease testing & updating

Content of a good Standard

- **Plan-Do-Check-Act approach.**
- **Mature and stable.**
- **Not contradicting or in conflict with corporate or international standards.**
- **Clear and easy to understand.**
- **Systematic.**
- **Realistic and practical.**
- **Solves all parts of the problem.**
- **Well structured and organized. Measurable.**
- **Has a clear accreditation and certification process.**
- **Widely followed and adapted.**

Some standards

- Widely recognized security standard is International Organization for Standardization/International Electrotechnical Commission [ISO/IEC 27002], consists of two basic parts i.e. BS 7799 part 1 and BS 7799 part 2.
- Both of these parts were created by British Standards Institute (BSI).
- Part 1 provides an outline or good practice guide for cyber security management
- Part 2 provides a framework for certification

Cont.

- ISO/IEC JTC 1 Subcommittee 27 Cybersecurity

- ISO/IEC 27017 – Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002

Pros and Cons of Having Standard

- Ease automation, facilitate better protection e.g. security updates
- Eliminate known security weaknesses
- Consistent practices ease recognition of expectation

- Mass deployment of weak or vulnerable security mechanisms
- Create false sense of security
- Slow to change
- Overlapping and intersection between standards.
- Overlapping and varying abbreviations and definitions.

abmunir@um.edu.my
http://profabm.blogspot.com
Mobile- 0122185242