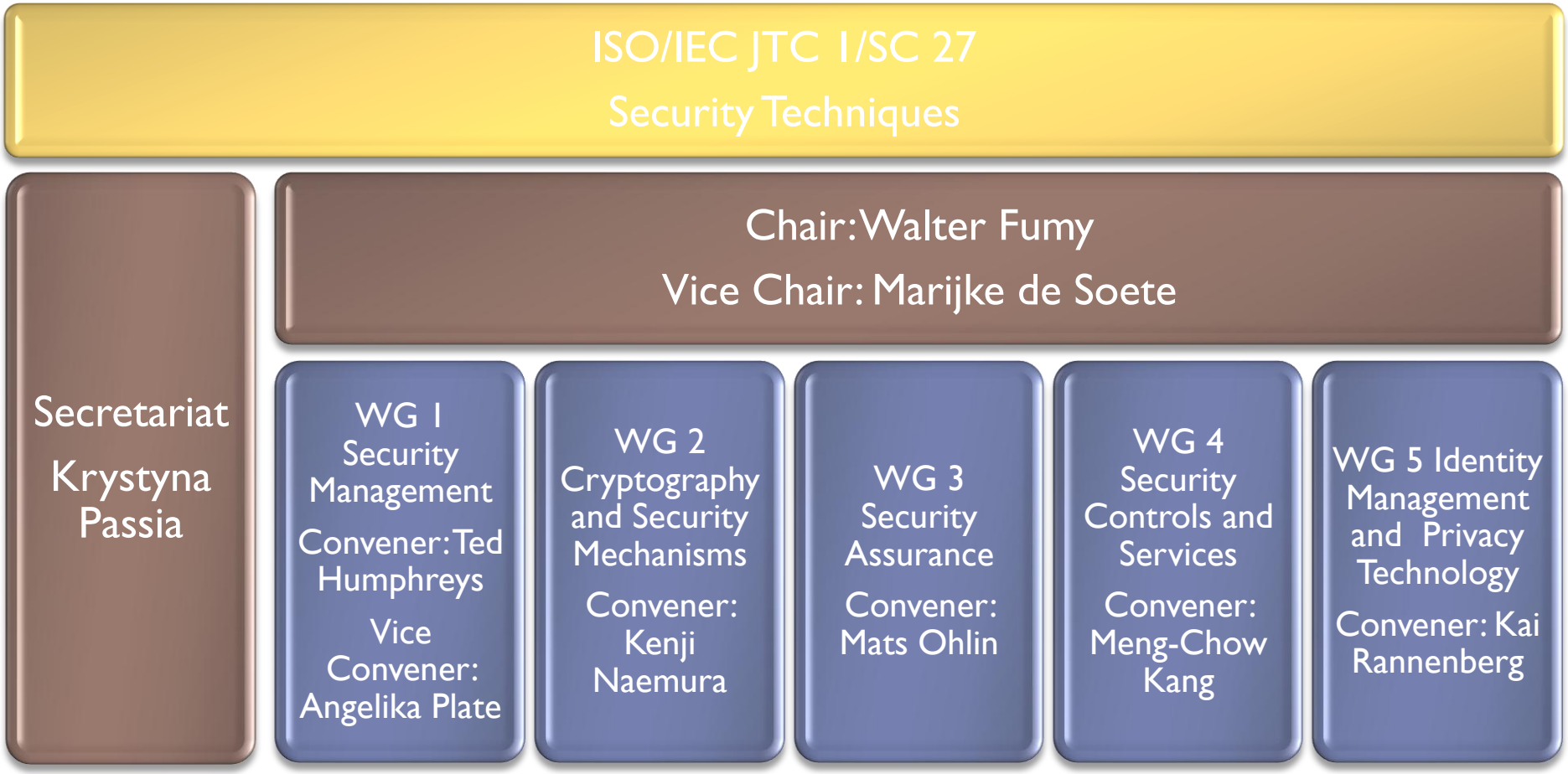
WG 4 Roadmap & Progress

Slides by Meng-Chow Kang, PhD, CISSP, CISA
Convener, ISO/IEC JTC 1/SC 27/WG 4 – Security Controls &
Presentation by ir. Alain De Greve, MCA, CISA
Expert, ISO/IEC JTC 1/SC27 wg1 & wg4 – coordination for Belgium 27000 series

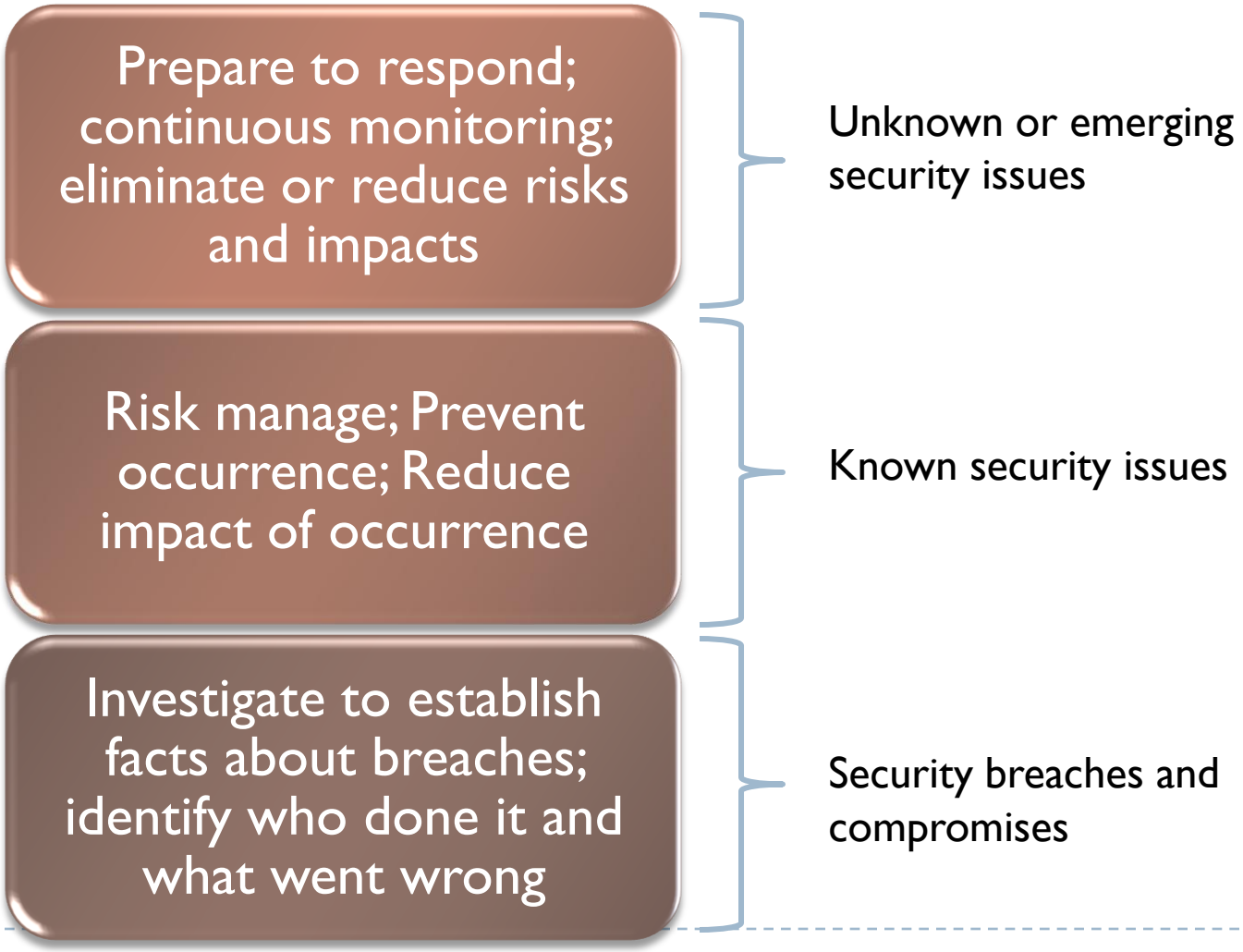
ENISA Workshop on Resilience

November 13, 2008

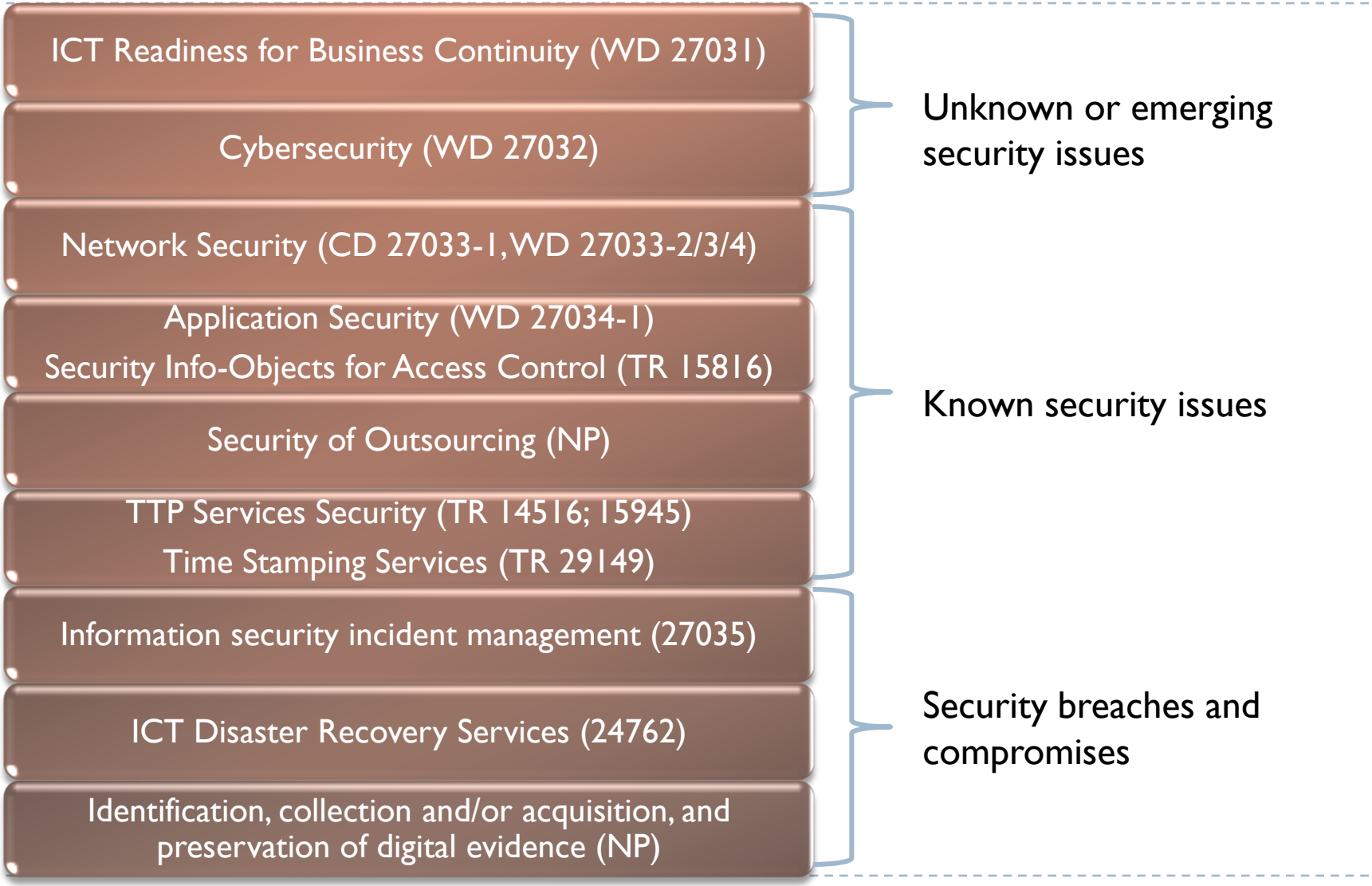
ISO/IEC JTC 1/SC 27 Organization



WG 4 Roadmap Framework



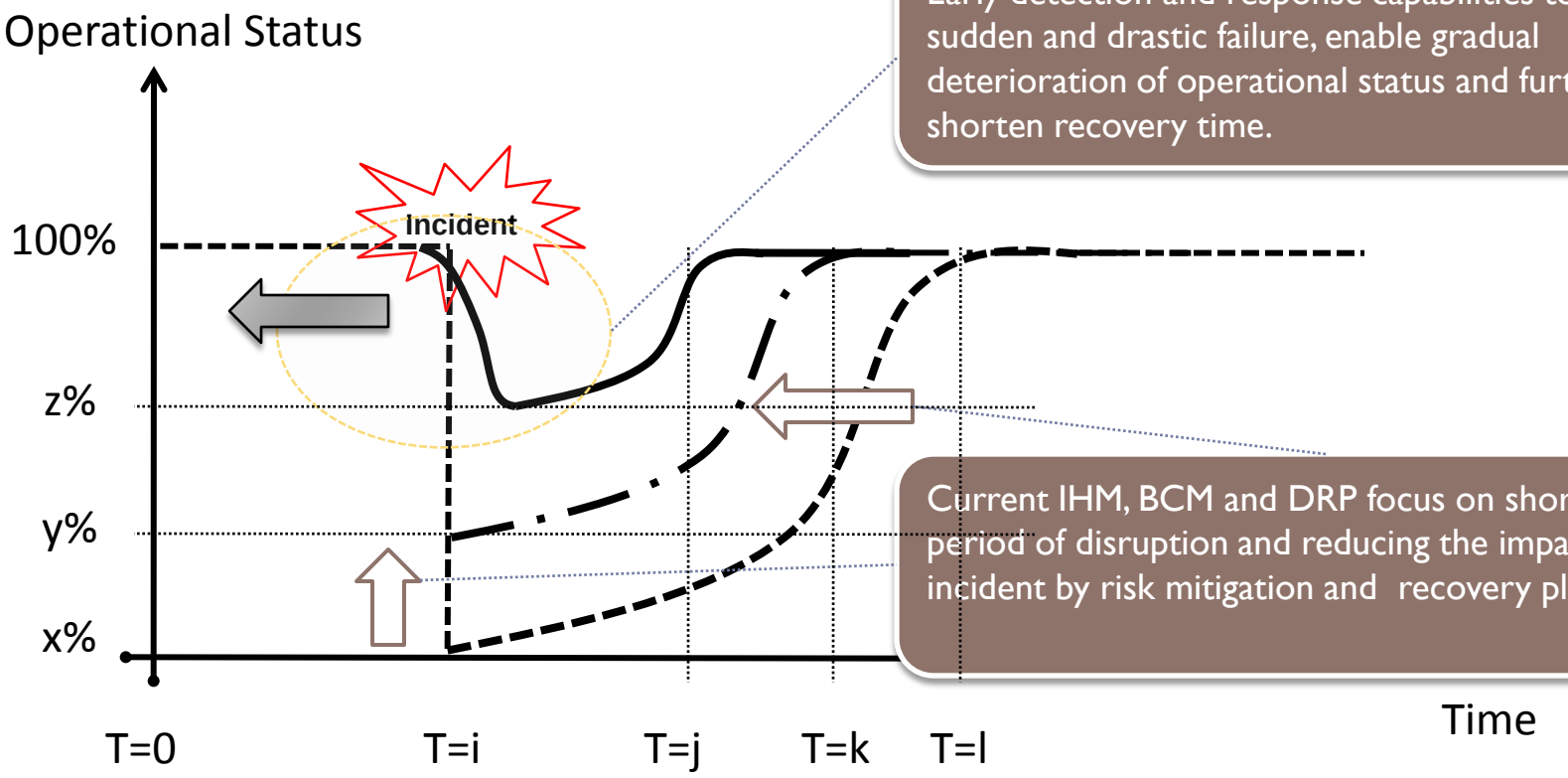
WG 4 Projects & Study Periods



ICT Readiness for Business Continuity (27031)

- What is ICT Readiness?
  - Prepare organization ICT technology (infrastructure, operation, applications), process, and people against unforeseeable events that could change the risk environment and impact ICT and business continuity
  - Leverage and streamline resources among traditional business continuity, disaster recovery, emergency response, and ICT security incident response and management
- Why ICT Readiness focus on Business Continuity?
  - ICT systems are prevalent in organizations
  - ICT systems are necessary to support incident, business continuity, disaster, and emergency response and management needs
  - Business continuity is incomplete without considering ICT systems availability and continuity
  - Responding to security incident, disasters, and emergency situations are about business continuity

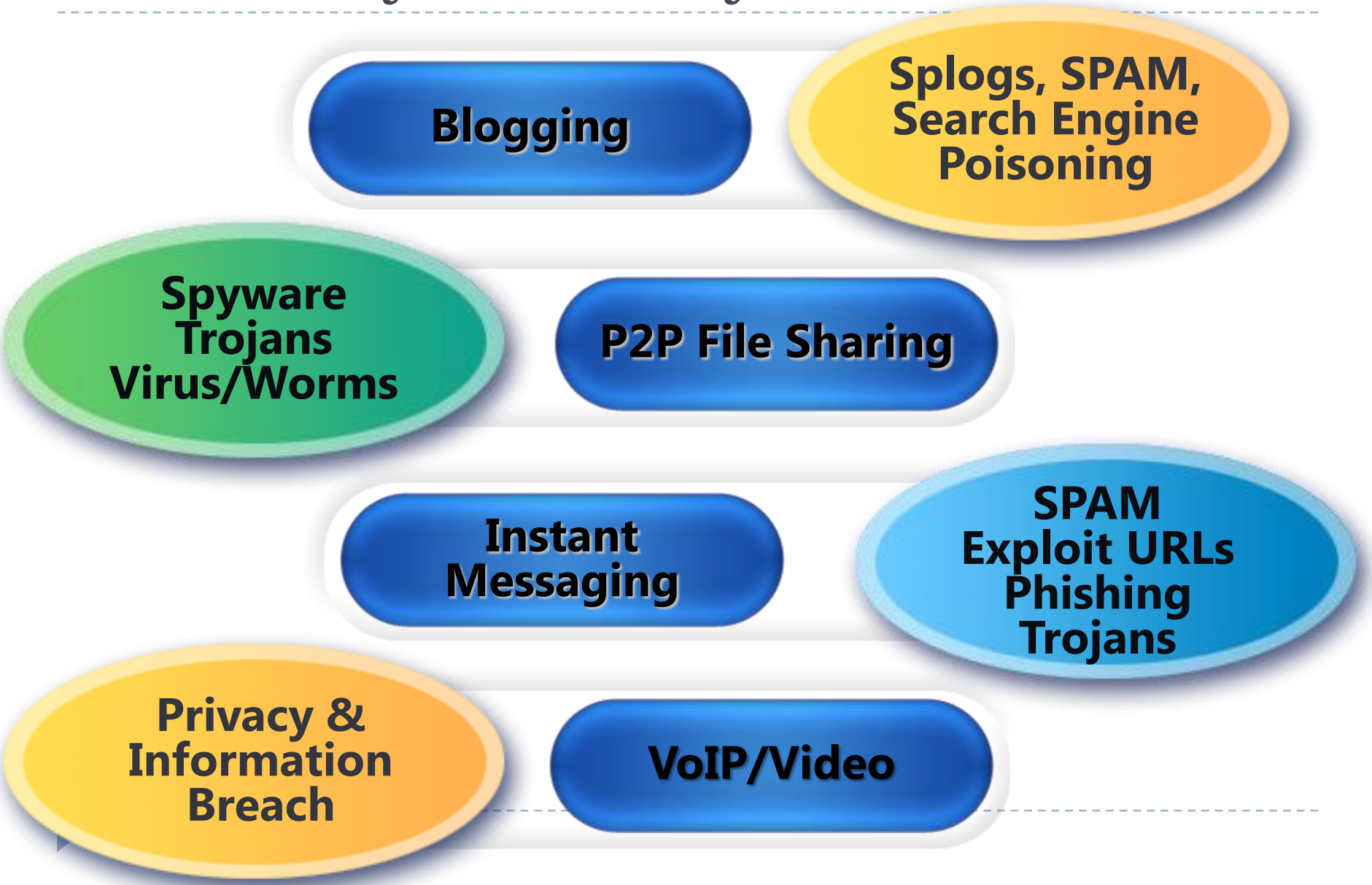
Implications of ICT Readiness



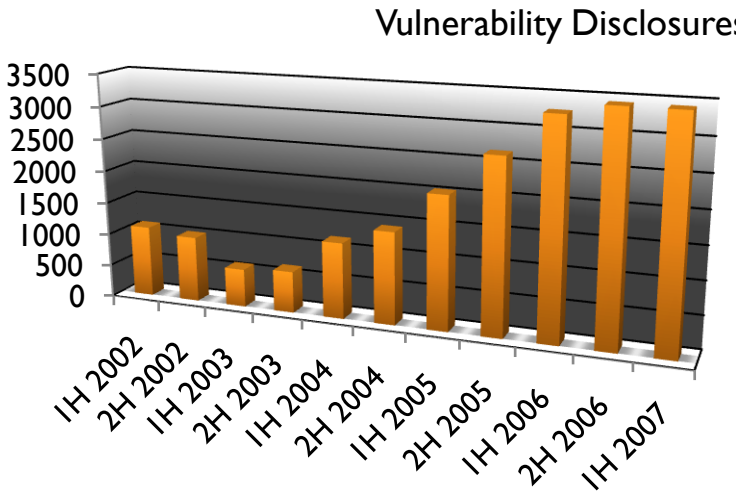
ICT Readiness for Business Continuity

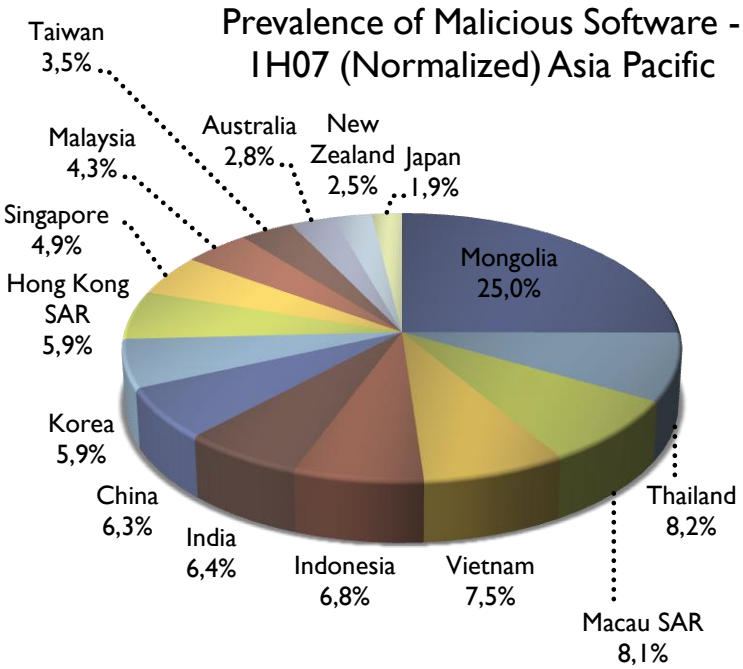
- Re-proposed as single-part standard (Nov '07)
- Approach
  - Based on PDCA cyclical model
  - Extend BCP approach (using RA, and BIA)
  - Introduce Failure Scenario Assessment (with FMEA as example)
  - Focus on defining and identifying Triggering Events
  - Management of IRBC Program

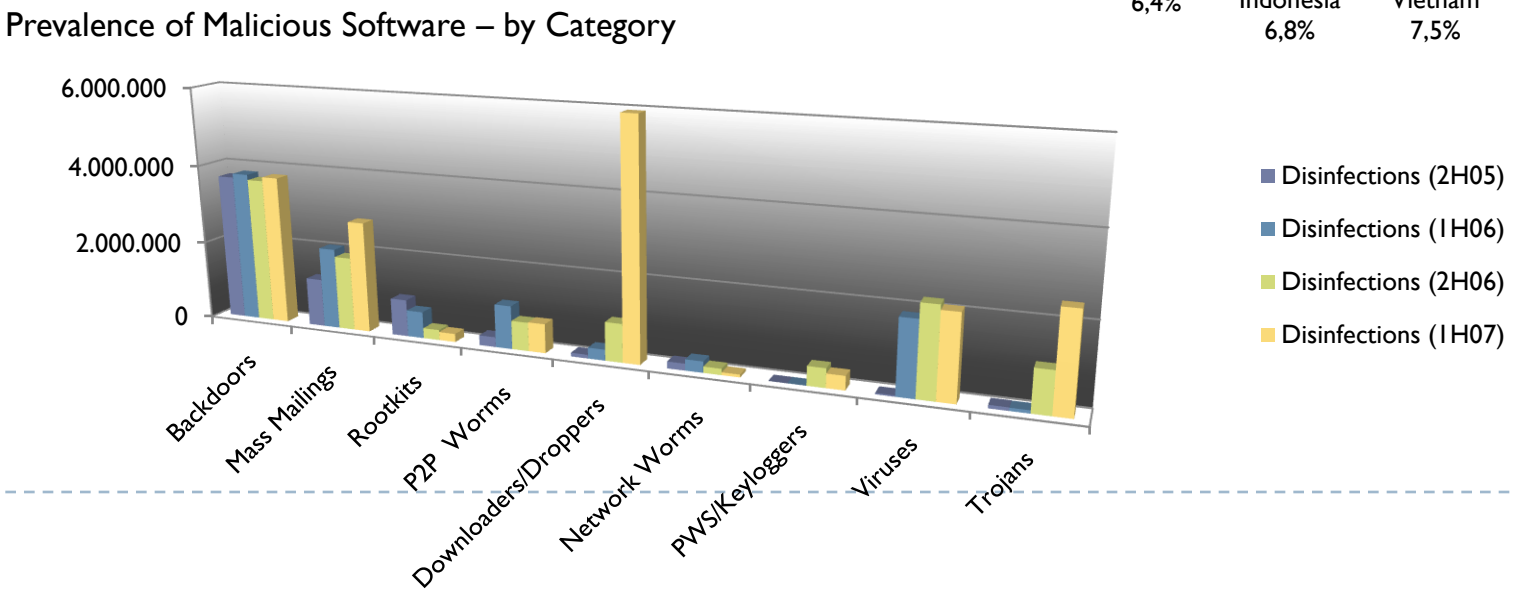
Web 2.0 Cybersecurity Issues



Global Threat Landscape







What is Cybersecurity

- Definition of Cybersecurity overlaps Internet/network security
- Nature Cybersecurity issues
  - Occurs on the Internet (Cyberspace)
  - Global nature, multiple countries, different policy and regulations, different focus
  - Multiple entities, simple client system to complex infrastructure
  - Weakest link and lowest common denominator prevail
  - Highly creative landscape – always changing

Cybersecurity

- Cyberspace, while not existing in any physical form, is a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it.
- The complex environment encompasses the interconnecting networks and systems as well as any ICT devices belonging to different organizations and service providers that allow for the flow of information.
- However, there are security issues that are not covered by current information security, Internet security, network security and ICT security best practices because there are gaps between these domains.
- Cyberspace security, or Cybersecurity, is about the security of the Cyberspace, providing guidance to address issues arising from the gaps between the different security domains in the Cyberspace environment while at the same time provide an infrastructure for collaboration.

Guidelines for Cybersecurity

- "Best practice" guidance in achieving and maintaining security in the cyber environment
  - an overview of Cybersecurity;
  - an explanation of the relationship between Cybersecurity and other types of information security;
  - a definition of stakeholders and a description of their roles in Cybersecurity;
  - guidance for addressing common Cybersecurity issues; and
  - a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

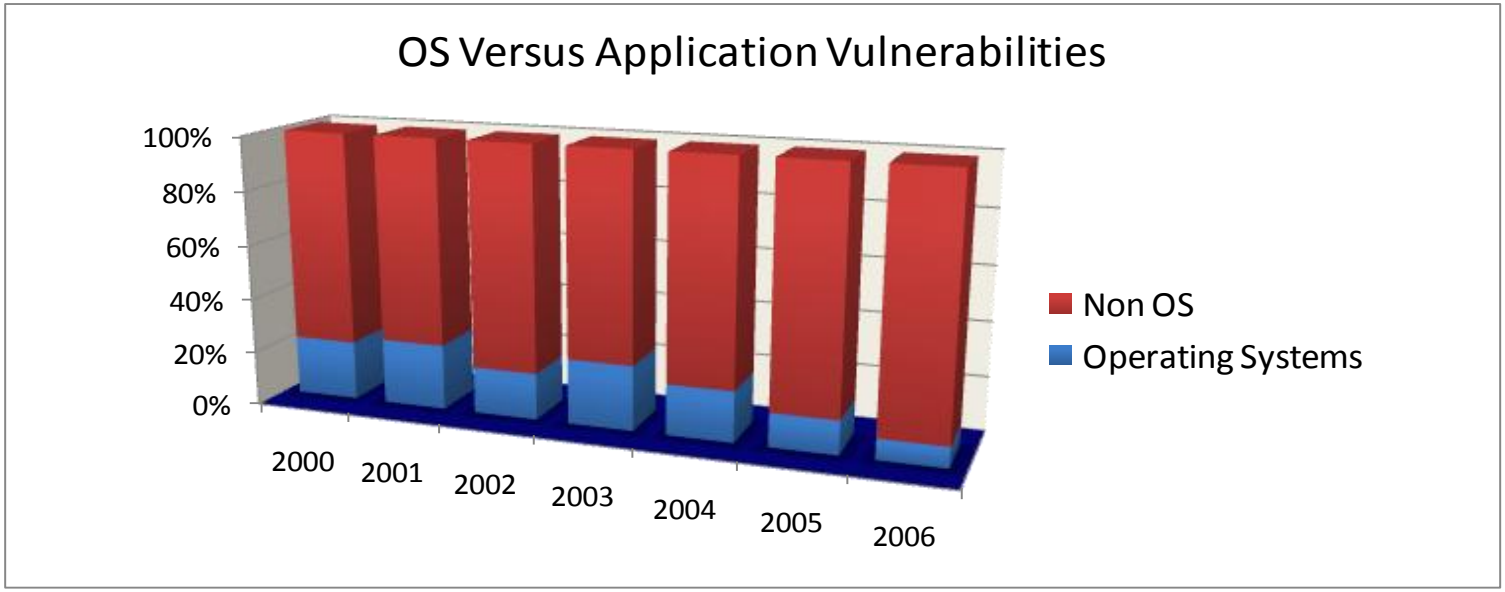
Network Security

- Revision of ISO/IEC 18028
- Re-focus, re-scoping, and new parts
  - Part 1 – Guidelines (Overview, Concepts, Principles)
  - Part 2 – Guidelines for Design and Implementation
  - Part 3 – Reference Networking Scenarios: Risks, Design, Techniques, and Control Issues
  - Part 4 – Security communications between networks using security gateways
  - Part 5 – Security communications between networks using Virtual private network
  - Part 6 – IP Convergence
  - Part 7 – Wireless

Software Vulnerability Disclosures

OS versus application vulnerabilities

- Application vulnerabilities continued to grow relative to operating system vulnerabilities as a percentage of all disclosures during 2006
- Supports the observation that security vulnerability researchers may be focusing more on applications than in the past



Guidelines for Application Security

- Reduce security problems at the application layers
- Eliminate common weaknesses at code and process levels
- Strengthen security of code base improve application security and reliability
- Multi-parts standards, including
  - Code Security Certification
  - Process Security Certification
- Code Security
  - Testing and certification per major release of application
- Process Security
  - Security Development Lifecycle
  - Assure security of code from design to operation, including minor releases, patch development & release
- Focus on Web-based applications (major problem areas)

Guidelines for Application Security

- Specify an application security life cycle, incorporating the security activities and controls for use as part of an application life cycle, covering applications developed through internal development, external acquisition, outsourcing/offshoring1, or a hybrid of these approaches.
- Provide guidance to business and IT managers, developers, auditors, and end-users to ensure that the desired level of security is attained in business applications in line with the requirements of the organization's Information Security Management Systems (ISMS).
- Application security addresses all aspects of security required to determine the information security requirements, and ensure adequate protection of information accessed by an application as well as to prevent unauthorized use of the application and unauthorized actions of an application.
- Informational security concerns in business applications are to be addressed in all phases of the application life cycle, as guided by the organization's risk management principles and the ISMS adopted.

Guidelines for Application Security

- Structure (DRAFT)
  - Part 1 – Overview, concepts, and principles
  - Part 2 – Application security management process
  - Part 3 – Architecture, design, and development
  - Part 4 – Protocols and data structure
  - Part 5 – Application security assurance
  - Part 6 – Security guidance for specific applications

Summary


Changing Risks
Changing Practices
Standards Guiding Desired Change
New Attacks
Responsible Behaviors
New Technology
Evolving Security Approach

Thank you

Q & A

- mengchow@microsoft.com
- alain.degreve@skynet.be