

# Standards for Cybersecurity

## The need for sector collaboration

Michael Harrop  
The Cottingham Group



# The Need for Standards

- o Standards development and the need for standards predates cybersecurity and Critical Infrastructure protection
- o The topic of standardization is clearly much broader than just cybersecurity or CNI protection
- o Cybersecurity and CNI protection demand more than just infosec and network security standards
- o Standards in general have a long history and touch most facets of our lives



ITU-T

# Chronology of Infosec Standards

- Information security (Infosec) and information management, as disciplines, are not new but cybersecurity and its standardization is relatively new and is still evolving
- Cybersecurity standards are pre-dated by
  - IT standards which are pre-dated by
  - Telco standards which are pre-dated by
  - Non-ICT standards
- (And the disciplines of Infosec and information management predate them all - at least 2000 years old and likely much older)



ITU-T

# Why Standards?

- They facilitate inter-working in open, multi-vendor environment
- Products can be subjected to independent public scrutiny and assessment process
- To protect investment over multi-generations of product
- Can provide a framework for consistent application of IT Security



ITU-T

## Why are standards important?

- They facilitate inter-working in open, multi-vendor environment
- Products can be subjected to independent public scrutiny and assessment process
- To protect investment



ITU-T

## Public and Private Sector View of Standards

- o Both the public and private sectors have a need for standards
- o In each case, the demand for standards is driven by their business requirements and objectives
- o Hence, their reasons for needing standards are often not aligned



# Roles of Public and Private Sectors

## Public Administrations

- Govern
- Make and uphold laws
- Defend the land and people
- Negotiate external agreements
- Deliver and administer public services
- Support internal administration/operations

## Private Sector

- Maximize return to stakeholders
- Primary objective is to sell products/services at profit
- Support internal administration/operations



# Private sector

- Needs standards to:
  - Support or drive competitive position (need to inter-work with other vendors' products)
  - Meet market demand for standards-compliant products
  - To support efficient internal operations
- No requirement for competitive procurement - can source from single vendor
- A supplier that is dominant can often set its own proprietary standards and use them to disadvantage other suppliers.



# Public Sector

ITU-T

- Usually requires open competitive procurement and this may result in mixed supplier environment
- Needs standards-based products to mitigate product incompatibilities
- Demands standards for the “public good” e.g. health, safety etc
- May have procurement policy or international treaty requirements for standards-based products and services



# The role of sectors in CIP

## Private Sector

- In most countries, much of the critical infrastructure (and CNI in particular) is owned & operated by the private sector
- Development, supply, maintenance and safe operation of infrastructure components
- Participation in community defence measures
- Collaborating with producers, authorities, peer sector organizations and incident response teams to help resolve incidents

## Public Sector

- National emergency planning - leading and coordination overall effort
- Monitoring threats & vulnerabilities
- Participate in national & international standards fora e.g. ISO, ITU, IETF.
- Public education and awareness
- Collaborating with private sector and incident response teams to coordinate response to problems



# Collaboration of Sectors

- Collaboration between public and private sectors is vital and is a key part of all national CIP strategies
- But we need to improve that collaboration in some areas



ITU-T

# Improving collaboration

- Need for improved trust relationships
  - Need a better trust model for CERTs so they can exchange info with each other with confidence
  - Need more consistency in provision of public CERTs (Who runs public CERTs? Who funds them?)
  - Need to make sure that information on threats, attacks & vulnerabilities gets to the people who can respond in timely way (Question both of trust and knowing who to tell)



## Improving collaboration - 2

- Better incident response from business:
  - Need to make sure that businesses report vulnerabilities and breaches to incident centres promptly
  - Need to make sure that business knows how to report incidents and to whom



## Improving collaboration - 3

- Need to reduce vulnerability due to private user end systems
  - Encourage better software (fewer bugs; proper configuration)
  - Encourage ISP filtering and better filtering tools



ITU-T

## Improving collaboration - 4

- We need metrics and research to support CNIs
  - Quality-of-service standards for networks and security services
  - Identification of criticalities and interdependencies
  - Vulnerability assessment
  - Performance measurement

## Role of Standards in CIP

- Standards can help in a number of areas:
  - Operational criteria
  - Consistent Security Management (Guidance, Best Practices)
  - Better (more secure and reliable) software through test suites and good practices
  - QoS and performance standards
  - Address new vulnerabilities resulting from e.g. NGN and convergence



# Contribution to Standards Development

- o Private sector contributes as developer and as direct user of standards (i.e. uses standards in development of products and services as well as internal operations)
- o Public sector participates as “consumer” of standards, an end-user of standards-based products and as facilitator (to help direct and prioritize standards work)



# Need for Collaboration

- Public and private sectors must collaborate to make sure their standards needs are understood and met
- This is particularly important in areas like infosec and CNI protection where governments play a lead role in protecting citizens, national information assets and critical infrastructures



ITU-T

## Why individuals and organizations participate in standards work

- to ensure product interoperability/stimulate product ideas
- to influence the process/drive the process forward
- to prevent bad things happening
- to support procurement actions
- to encourage cross-pollination of ideas and thinking



ITU-T

## Why individuals and organizations participate - 2

- o to gain knowledge/understanding of developments
- o to provide insight for early adopters
- o to raise the profile of the organization/buy influence
- o to promote national/organizational interests/needs
- o to establish contacts with an international network of recognized experts



ITU-T

# What limits participation?

- o Most large public and private sector organizations claim to support standards work and many participate
- o However, under pressure (e.g. downsizing, cost-cutting etc) standards participation is often reduced or eliminated
- o This can have serious consequences



# An industry case study example

- o Large Canadian telecom manufacturer
- o Annual revenue was \$1.3BCdn and R&D budget \$150m Cdn.
- o They disbanded standards group of 8 people
- o Backed out of standards work
- o Quickly paid the price - cost \$8000 per problem in the field - problems they would have avoided if they had been aware of what was happening in standards development
- o Restructured and re-instituted stds program



ITU-T

# Misconceptions about Standards

- o “standards limit flexibility”
- o “standards increase the cost”
- o The marketplace has proved both the above to be wrong.



# The problem with IT standards

- o The formal processes are (necessarily) slow
- o It is difficult to develop standards fast enough to keep up with technology
- o It is difficult to achieve the right balance between prescriptiveness and flexibility



# The solution

ITU-T

- We need the formal standards processes for due process and long-term stability
- We need the informal processes of the IETF and the Open Source movement
- We the consortia to get rapid agreement on particular industry standards
- These organizations need to work together to develop credible standards quickly while avoiding duplication
- Both the public and private sectors need to participate to make sure this happens



ITU-T

## Elements for successful standards strategy

- *There must be senior management support*
- *The standards program and participation must be clearly in support of business goals*
- *All activities must be fully justified*
- *There must be accountability*
- *There must be broad participation in the organization*
- *Let the technical experts develop the contributions*
- *Establish central coordination and ensure effective information dissemination*



ITU-T

## It's not all about standards

- There is a need not only for collaboration, there is a vital need for trust
- In IT security and particularly in Critical Infrastructure protection, we are dealing with some highly sensitive information.
- How can we establish a high degree of mutual trust?

# Summary



- o Standards are critical for infosec and for CNI protection
- o Direct standards participation by public and private sector organizations is very important for the organizations and for the benefit of the community at large
- o Public/private sector collaboration is essential in areas like CIP and to make sure required standards are developed in a timely manner but how do we ensure mutual trust?



*Thank you*