UNECE – United Nations Economic Commission for Europe
UN/CEFACT – UN Centre for Trade Facilitation and e-Business

E-Government Domain Cybersecurity Workshop

(27 April 2016)

Vice Chair UN/CEFACT: Tahseen Khan

Domain Coordinator: Eric Okimoto

Agenda

- Cybersecurity 101
- Actors
- Targets
- Cyber Trends
- Information Security Keys
- Data Protection and Privacy
- Top 10 Points for Improving Cyber security posture (one of many)
- E-Commerce and Trade Precedence
- International Standards
- GROUP DISCUSSION
  - Cybersecurity areas of concern that would benefit from UN/CEFACT standards, guidance, or direction
  - Formalize project intent, anticipated outcomes, timeline, and group participation

Cybersecurity 101

Malware	• software that damages or disables computer systems (viruses, worms, Trojan horses, and spyware)
Phishing	• Where the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity
BOTNET	• A collection of independent computers that have each been hacked by a cyber criminal who uses them as a group to carry out malicious attacks .
Advanced Persistence Threat	• A network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time to steal data.
Attack Vectors	• The path by which a hacker gains access to a computer or network server in order to deliver a malicious outcome. Attack vectors exploit system vulnerabilities.

Cybersecurity Actors


Nation State

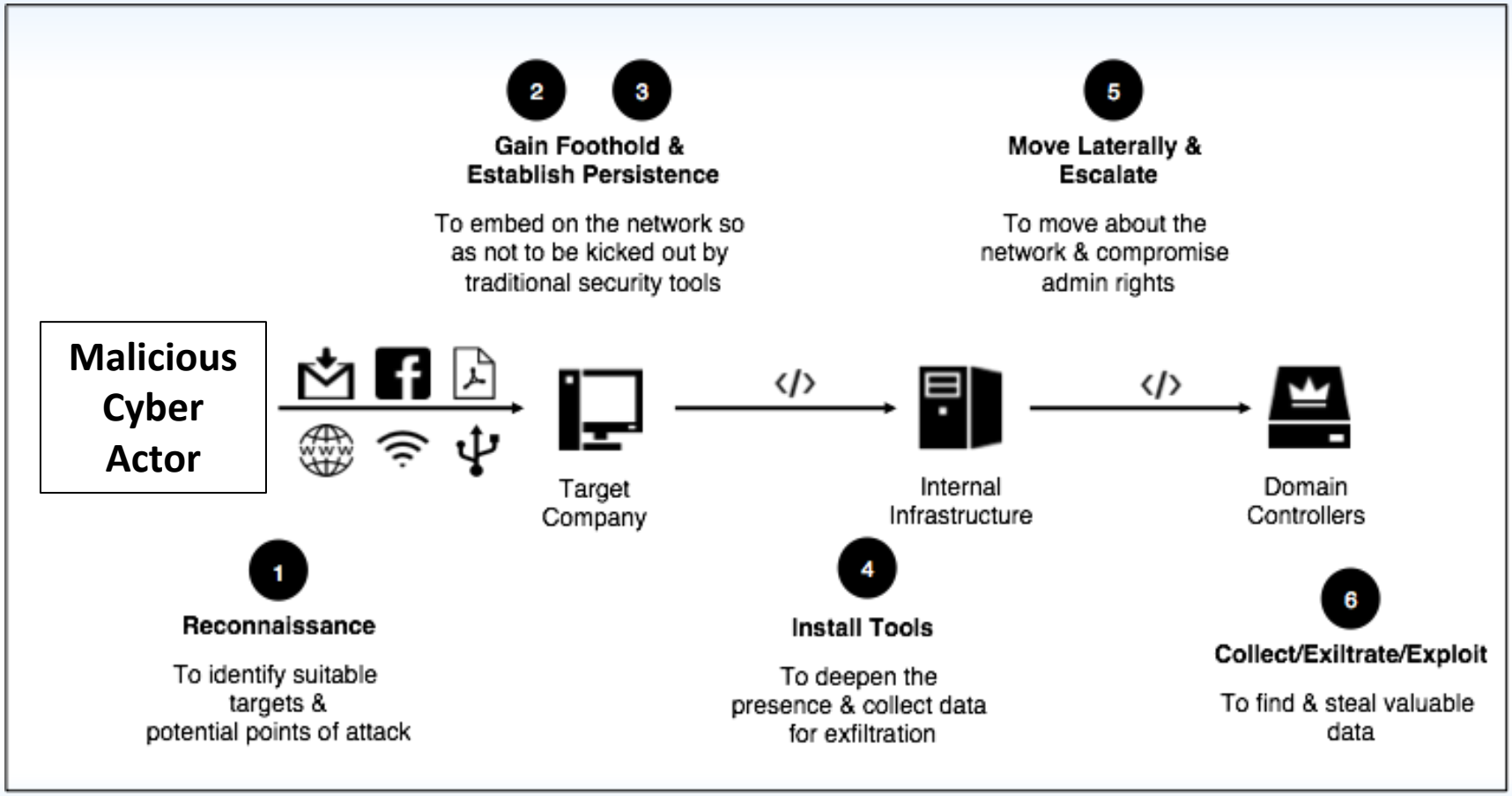

Organized Crime


Hacktivists


International Terrorists

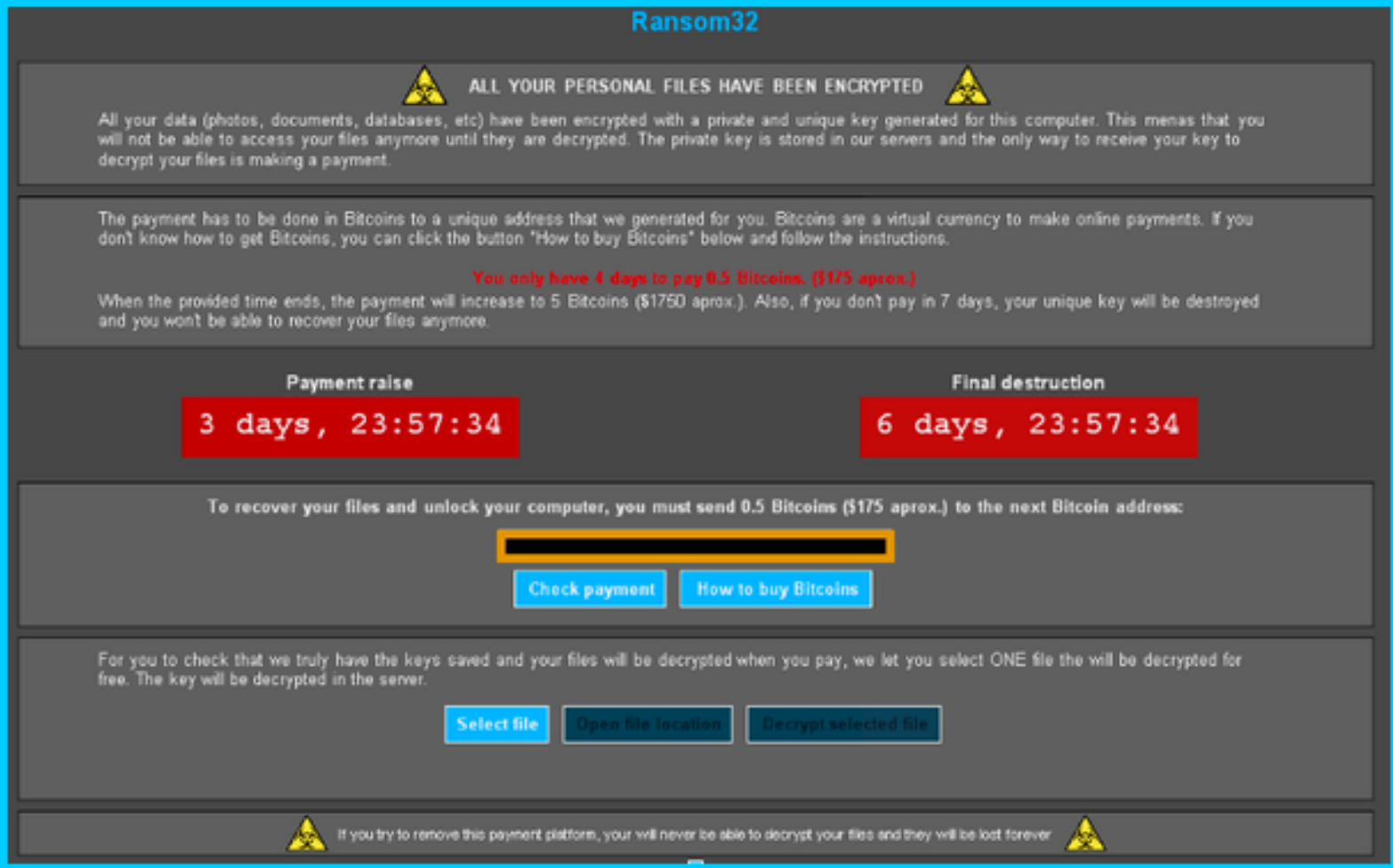

Insider Threats

Cyber Actors use cunning and advanced resources to exploit human errors



Source: Nisos Group

The result may cost you or your organization dearly….

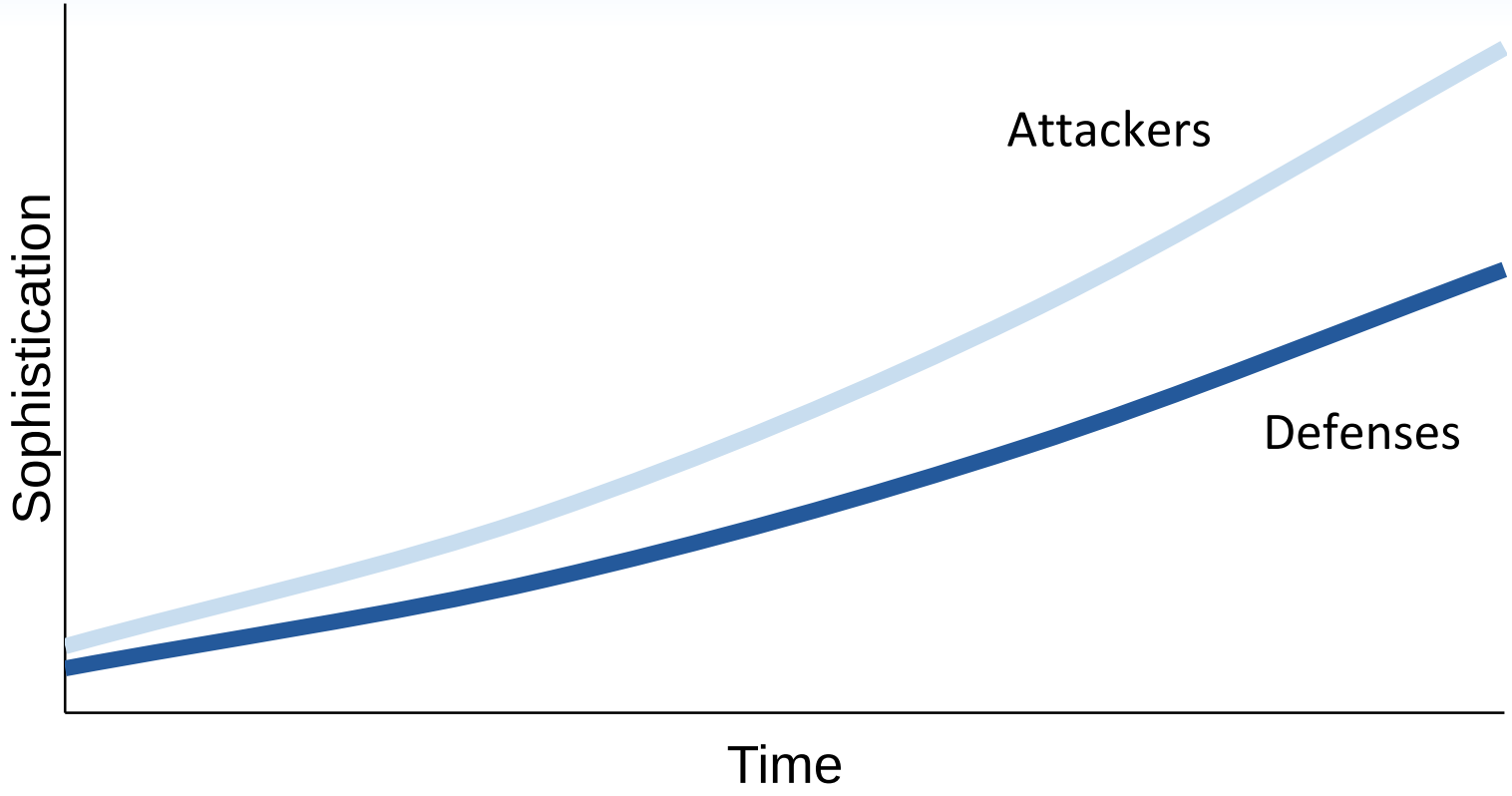


Source: Nisos Group

What is being targeted?

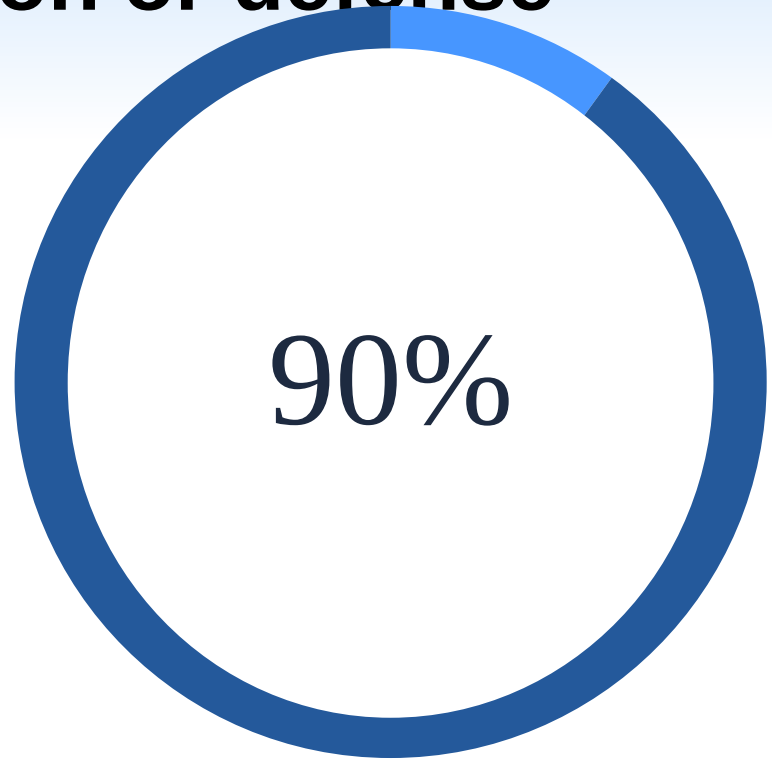
Transportation Control Systems and Logistics Information Management Systems	Supply Chain and Distribution Data	Payment Card and Financial Information
Industrial Control Systems	Health Records, Healthcare, and Pharmaceutical Information	R&D and Product Design data
Corporate Intel, Strategy, and M&A Data	Advanced Manufacturing Techniques and IP	IoT Endpoint Data – Sensors, Vehicle, Aviation

Attackers are Innovating Faster than cyber defenses…



Source: Nisos Group

Customized Attacks mean that there is no simple automated solution or defense



90% of the malware used in successful breaches in 2015 were unique to the attacked organization

Source: Verizon 2016 Data Breach Investigations Report

Cyber Trends

Dark Web

- Websites that use anonymity tools like Tor (the onion router) to hide their IP address
- Famous for black market commerce (silk road)
- Insider threat data (sysadmin username and passwords) is bought and sold on the dark web
- Knowledge Management system for bad cyber actors

Bitcoin

- Digital currency that relies on blockchain
- Used extensively in the dark web
- Mining for Bitcoins has become a driver of Botnets

Cyber Trends (cont.…)

Blockchain

- A distributed database that serves as a public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as 'completed' blocks are added to it with a new set of recordings.

IoT (Internet of Things)

- the ever-growing network of physical objects that feature an IP address for internet connectivity
- 25 billion devices are expected to be connected by 2015 and 50 billion are slated to connect by 2020
- Hackers are increasingly focusing on IoT vulnerabilities

Mobile

- Hackers are increasingly designing malware for mobile operating systems
- Mobile Financial Services are increasing and attracting hackers

"Because that is where the money is"

– Willie Sutton in response to a reporter asking him why he robbed banks

Key Security Principles

Confidentiality

- the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes

Integrity

- maintaining and assuring the accuracy and completeness of data over its entire life-cycle.

Availability

- information is available when needed (e.g. no denial of service)

Accountability (Non-repudiation)

- Ability to prevent an entity from later denying that they falsely performed (or did not perform) an action.

Source: ISO 27001 and ITU

Digital Identity and Access Control

Identification	• Who are you?
Authentication	• Confirm you are who you say you are
Authorization	• Once confirmed, you can access the following areas and see certain data/information

Data Protection and Data Privacy

Data Protection

- Identifies and classifies the data that an entity possesses or controls
- Maintains an understanding of where the data is
- Assures the legitimacy of data handling
- Assures the adequacy of safeguards

Privacy is the appropriate use of personal and sensitive data under the circumstances. What is appropriate will depend on the context, law, and the data subject's expectations; also, the right of the data subject to control collection, use and disclosure of the data. (IAPP)

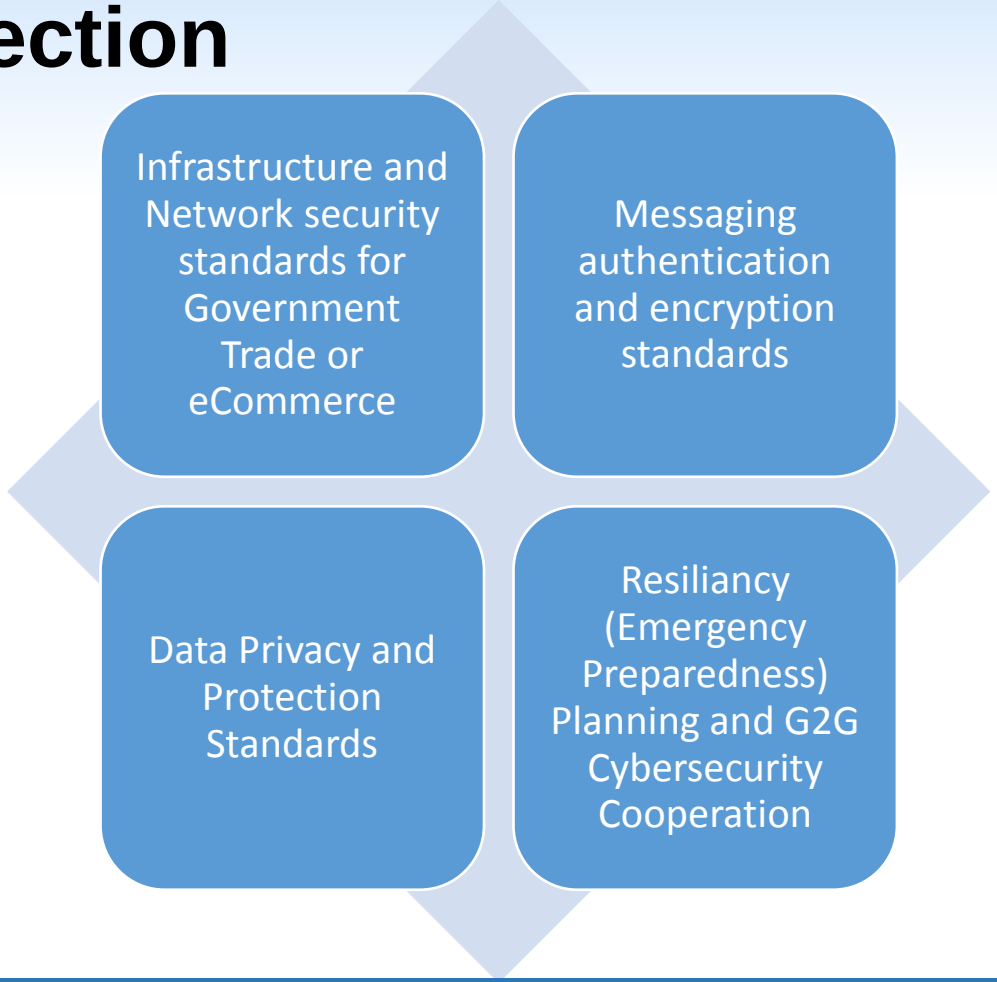
E-Commerce and Trade Precedence

WTO	• GATS Article XIV Governs some online privacy protections for eCommerce, illegal or illicit content, and cyber crimes and fraud
WEF	• Focused efforts on building cyber resilience (emergency preparedness) in supply chains
TPP	• eCommerce consumer protection from fraud and deceit • Protection of personal information of online consumers • Cybersecurity cooperation
WCO	• No major cyber efforts to date

International Standards

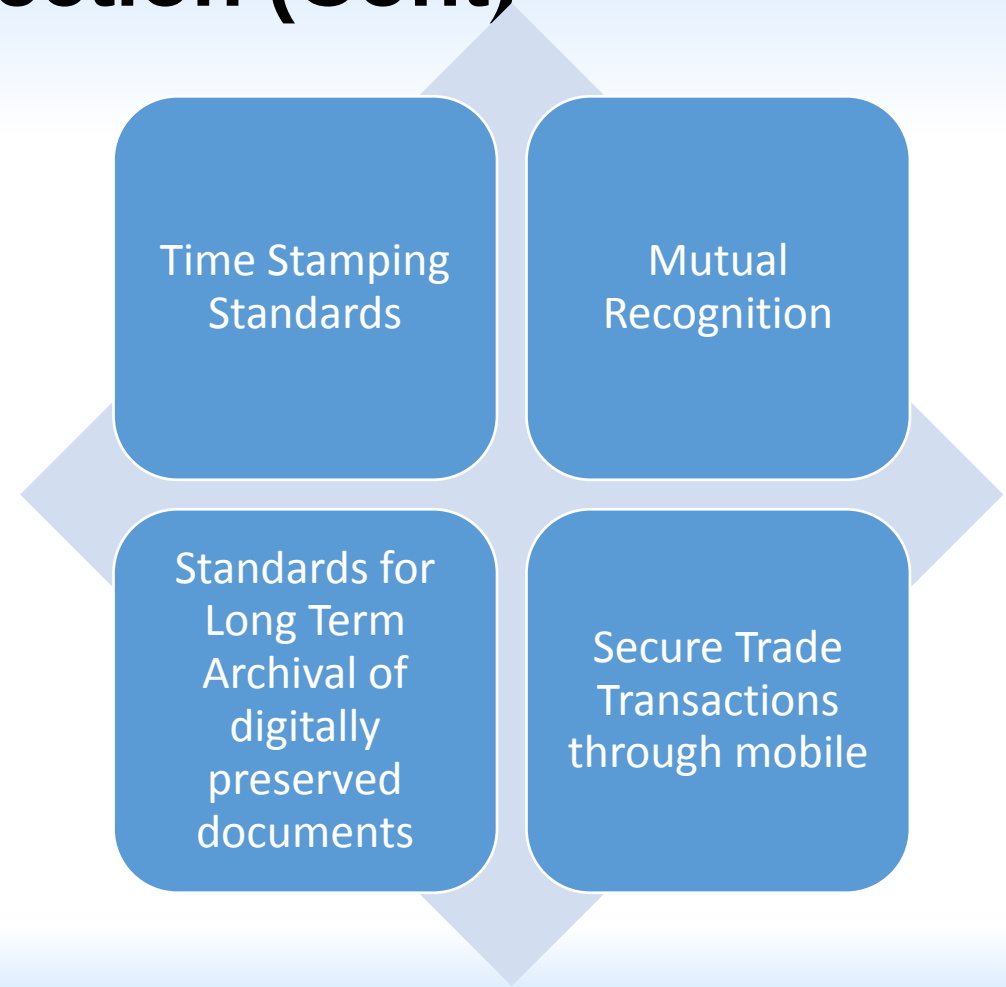
- ISO 27001 – Controls
- ISO 27002 – Guidelines for Implementation
- ISACA – Information Systems and Audit Control Association
- IAPP – International Association of Privacy Professionals
- SANS – Information Security Training
- PCI DSS – Payment Card Industry Data Security Standard
- OECD – Guidelines for the Security of Information Systems
- ITU – UN Guidelines on cybersecurity (SG17)

Possible areas of standards, guidance and UN/CEFACT direction



ITU has established the technical standards….the UN/CEFACT should focus on guidance that enables trust and manages cybersecurity risks to eCommerce and Trade

Possible areas of standards, guidance and UN/CEFACT direction (Cont)



Group Discussion

Questions for Group

- What topics or areas are of most interest and relevance?
- What efforts on suggested topics have been put forth previously by other teams?
- Prioritize topic areas
- Discuss methodology and way forward:
  - Confirm topics
  - Develop topic concepts
  - Develop white papers for socialization

eGOV Domain Open Discussion

Aside from cybersecurity, what topics of interest exist within the eGOV Domain?

Thank You!

Ericjamesokimoto@gmail.com