NTRA
National Telecom Regularity Authority
الجهاز القومى لتنظيم الإتصالات

ITU

ITU Workshop Smart Sustainable Cities
(Samarqand - Uzbekistan 1- 2 June 2017)

Trustworthy ICT:
The notion of Trust, Security, and Privacy

Ramy Ahmed Fathy, PhD

Vice Chairman of ITU-T SG20

Director, Digital Services Planning and Risk Assessment

Content

- Complexity of Trust
- The Concept of Trust
- Theoretical Framework of Trust
- How big is the risk? And how real is it?
- Relationship to Privacy
- Recommendations and Trustworthy ICT Generic Requirement

Content

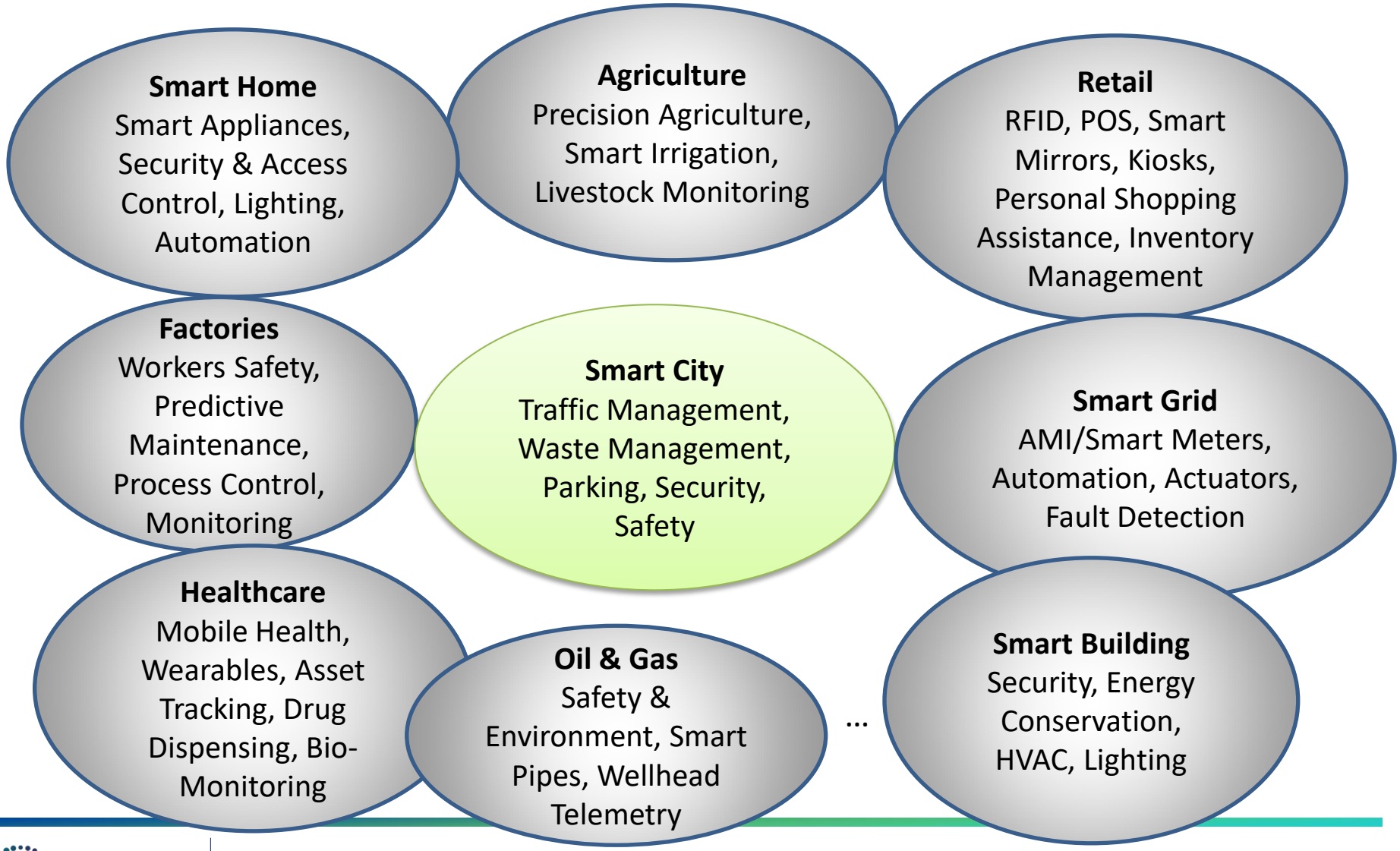
- Complexity of Trust
- The Concept of Trust
- Theoretical Framework of Trust
- How big is the risk? And how real is it?
- Relationship to Privacy
- Recommendations and Trustworthy ICT Generic Requirement

What is the problem? The threats and attack vectors are huge.

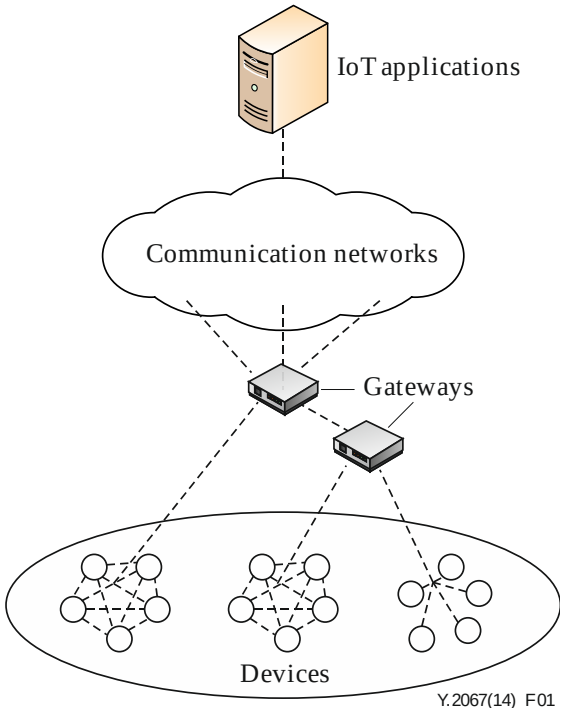
Let us have a closer look at the things.. They are simply every object on the planet! Data are immense!

- Smart phones
- Laptops, PCs,..
- Home appliances
- CCTV cameras
- Wearables
- Medical equipment
- Cars
- Software agents
- Web services
- Robots
- Drones
- Sensors
- Valves

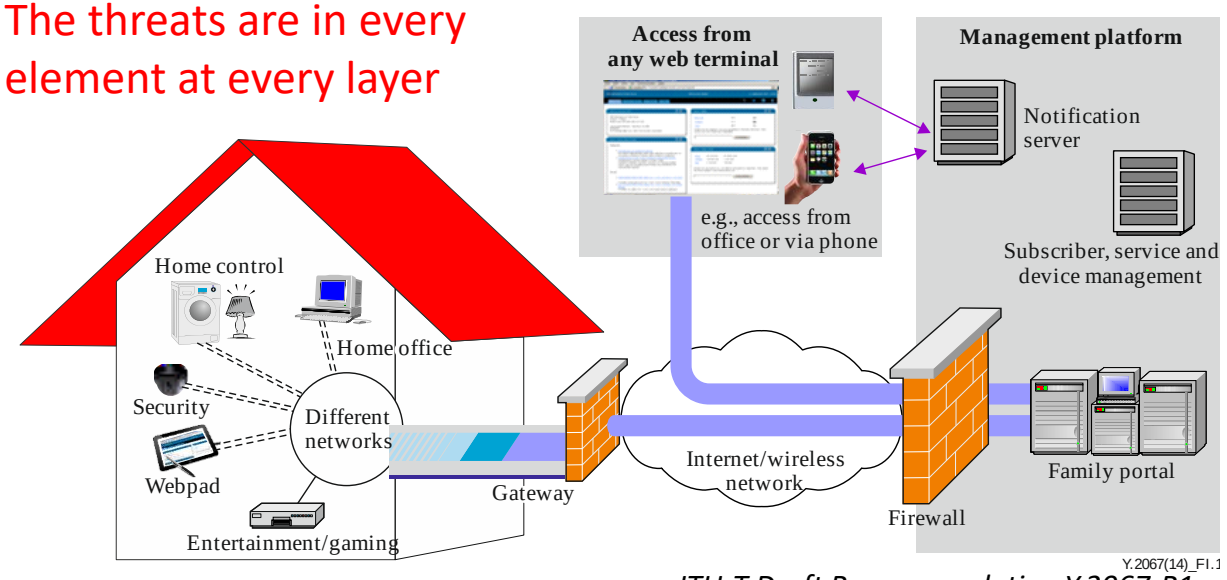
More than a dozen application and service domains = Domains of Opportunities.. Risks.. Security Concerns.. Privacy.. Trust..



To look at system threats (e.g. IoT), you need to look at its elements!



The threats are in every element at every layer



ITU-T Draft Recommendation Y.2067-R1

Different applications and services have different characteristics and requirements. → More complicated security & privacy measures.

Example Applications	Data volume	Quality of Service	Amount of signaling	Time sensitivity	Mobility	Server initiated Communication	Packet switched only
Smart energy meters	low	low	intermediate	very low	no	yes	yes
Road charging	low	low	low	low	yes	no	yes
eCall	very low	very high	very low	very high	yes	no	no
Remote maintenance	low	low	high	high	no	yes	yes
Fleet management	low	low	very high	intermediate	yes	yes	no
Photo frames	intermediate	low	high	low	no	yes	yes
Assets tracking	low	low	very high	high	yes	yes	no
Mobile payments	intermediate	low	high	very high	yes	no	yes
Media synchronisation	high	low	high	intermediate	yes	yes	yes
Surveillance cameras	very high	very high	very low	very high	no	yes	yes
Health monitoring	high	high	high	very high	yes	yes	yes

very low | low | intermediate | high | very high

Source: *Handbook: Impacts of M2M Communications & Non-M2M Mobile Data Applications on Mobile Networks*, page 50. ITU (Geneva, 2012). Available at: www.itu.int/md/T09-SG11-120611-TD-GEN-0844/en.

Conclusion so far.. Lesson #1

- Threats are expected to be huge, highly probable and highly diversified.
- Threats are expected to target hardware, protocols, and information systems components.
- Threats are application specific.
- Risk assessment and impact analysis should be administered by application domains subject matter experts.
- Interoperability is problem, and a probable weak point.

Trustworthy ICT

- But Trust.. It is a far more complex concept!
- Trust is a complex concept which involves interactions between several domains like phycology, cognitive sciences, security, and anthropology.

- i.e. Other domains of complexity are added..

Content

- Complexity of Trust
- The Concept of Trust
- Theoretical Framework of Trust
- How big is the risk? And how real is it?
- Relationship to Privacy
- Recommendations and Trustworthy ICT Generic Requirement

There is a say.. Security is as strong as its weakest link.. So is trust!

The Cliffhanger, 1993)

What is trust? There is no common definition!

- Trust is the belief that the trustee will behave according to our expectation.
- Trust is the perceived credibility and benevolence of a target of trust.
- It is the propensity of the trustor to take the risk of trusting the trustee.
- The trustor's decision is based on both cognitive and affective appraisal of existing information about the trustee, either statically available or dynamically derived from the observation of the trustee's behavior in a medium-long term interaction.

Challenges in defining trust lies in the fact that there is no agreement on how to distinguish between the antecedents of trust & the construct of trust itself.

- Costa, Roe, and Tail-lieu (2001) conceptualized trust as a multi-component variable with three distinct but interrelated dimensions.

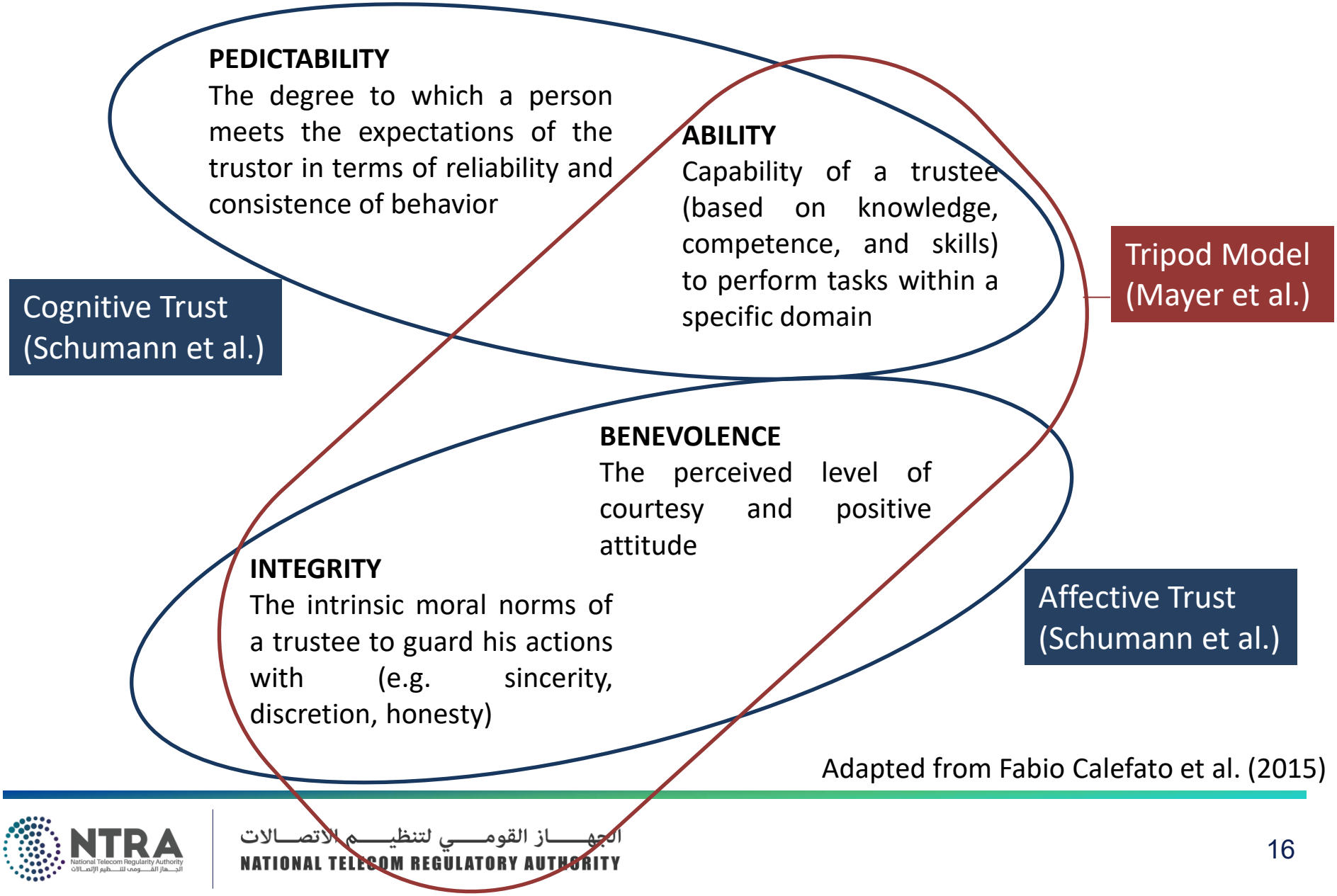
- These dimensions consist of propensity to trust, perceived trustworthiness, and cooperative and monitoring behaviors.

- This definition includes a dispositional variable, propensity to trust, as well as cognitive and behavioral dimensions.

Content

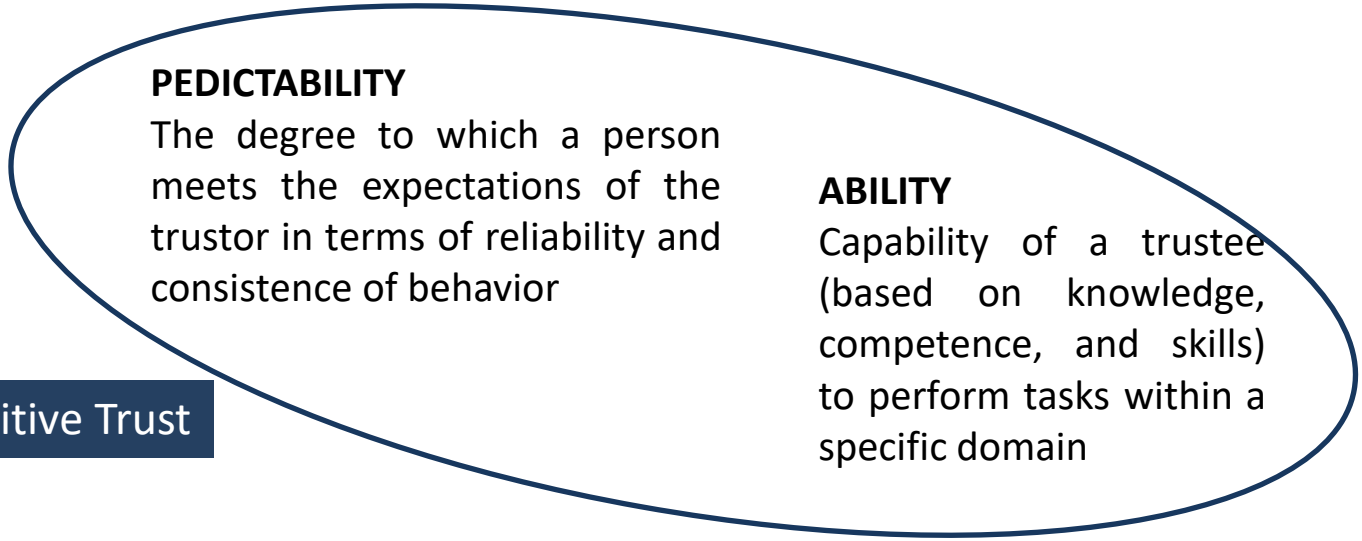
- Complexity of Trust
- The Concept of Trust
- Theoretical Framework of Trust
- How big is the risk? And how real is it?
- Relationship to Privacy
- Recommendations and Trustworthy ICT Generic Requirement

Antecedents of Trust: Theoretical Framework



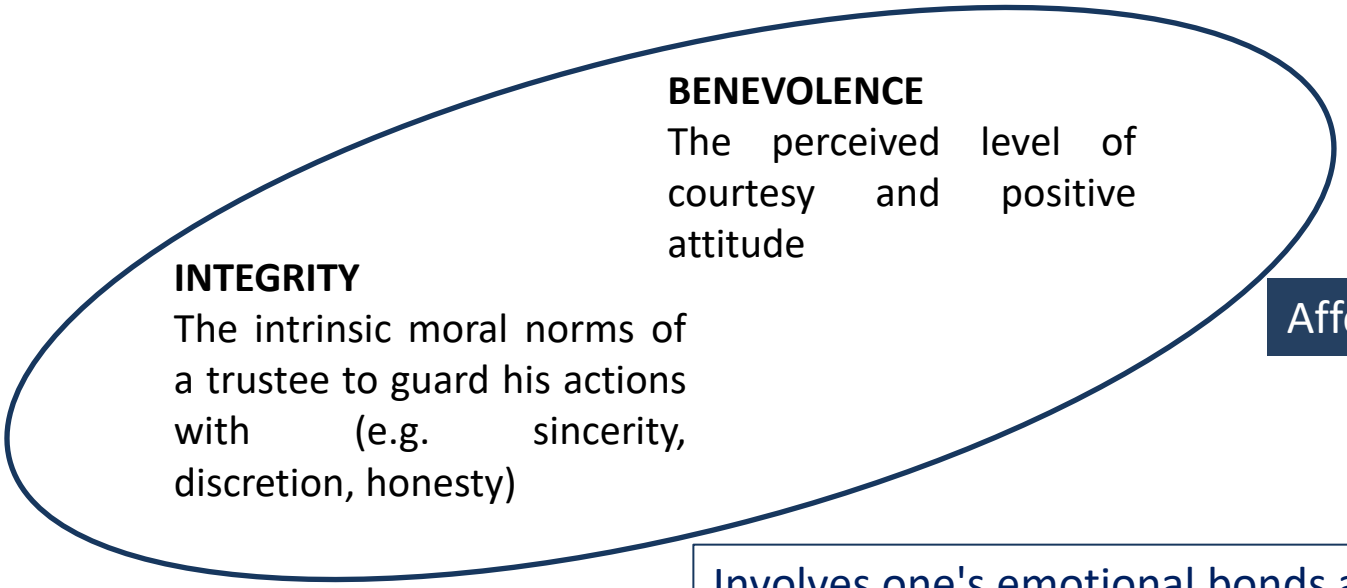
Adapted from Fabio Calefato et al. (2015)

Two Dimensions of Trust (1): Cognitive Trust



Results from deliberate assessment of other's characteristics and the process to weighing benefits of trusting over risks

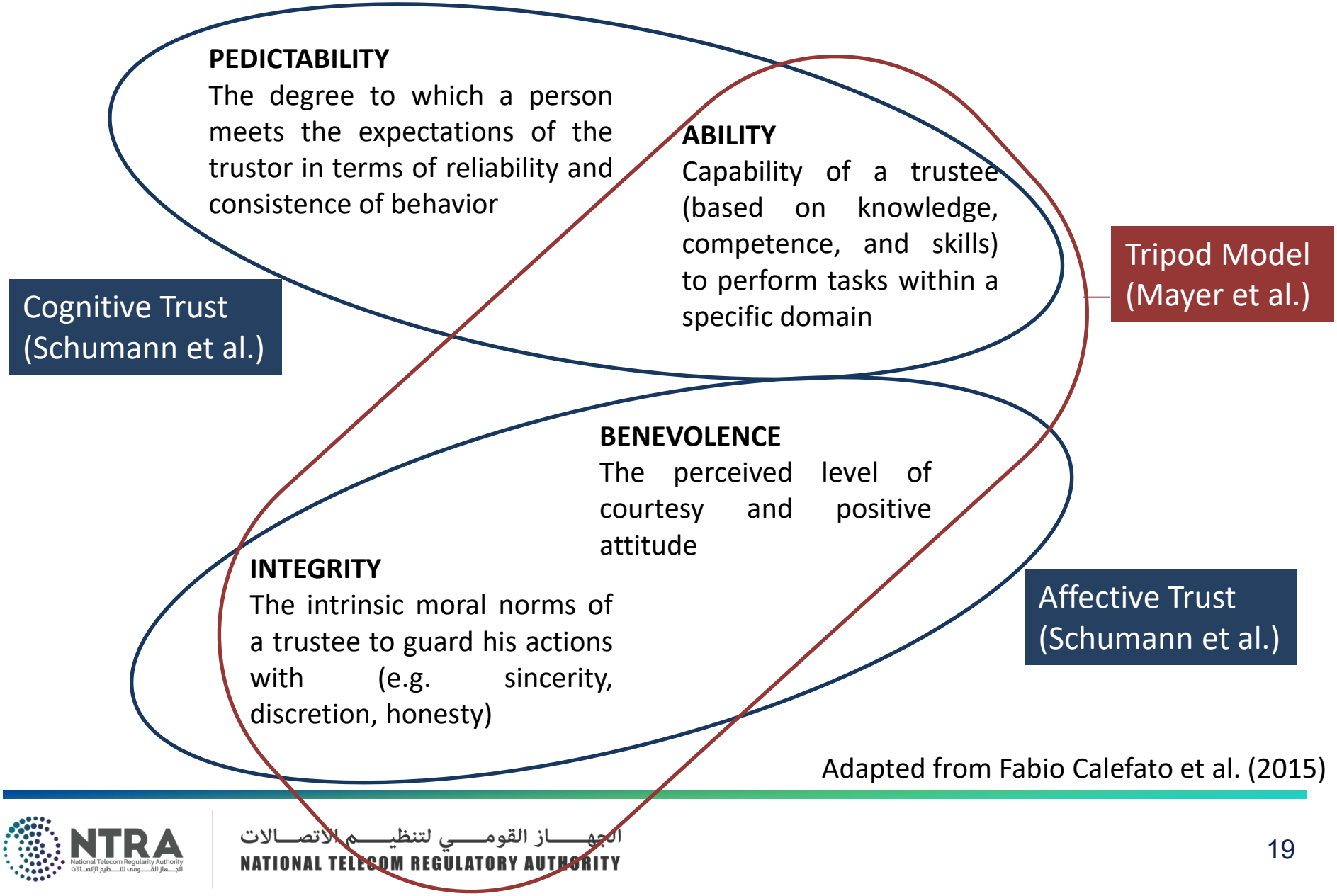
Two Dimensions of Trust (2): Affective Trust



Affective Trust

Involves one's emotional bonds and sincere concern for the well being of the others

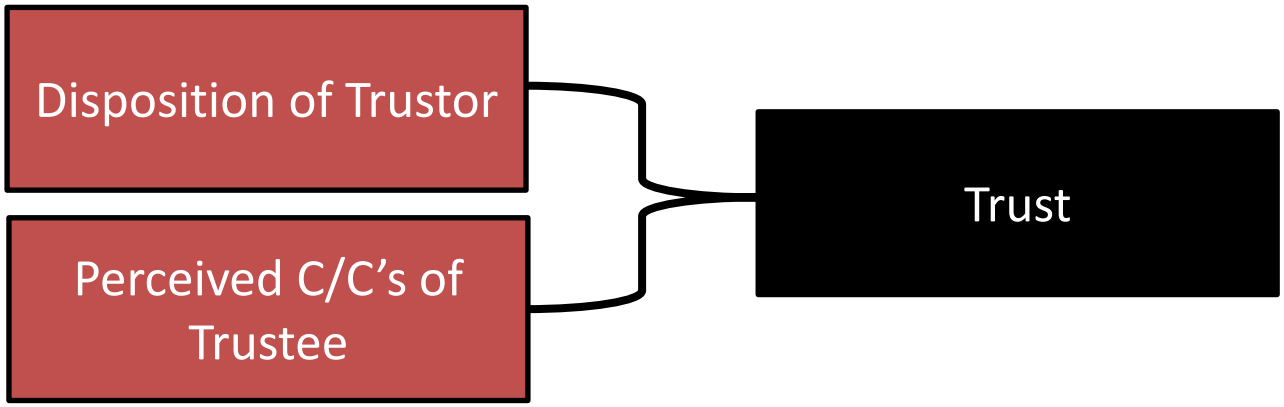
Antecedents of Trust: Tripod Model assumes three components



Adapted from Fabio Calefato et al. (2015)

Tripod Model

- Trust is ‘‘the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party’’



Mayer et al. (1995)

Tripod Model (2)

- Trust represents an intention to take a risk in a relationship
- Beliefs in the trustee's ability (knowledge, skills, and competencies)
- Benevolence (the extent to which a trustor believes that a trustee will act in the best interest of the trustor)
- Integrity (the extent to which the trustor perceives the trustee as acting in accord with a set of principles that the trustor finds acceptable).

McKnight's Model extended the Tripod model by adding the predictability concept..

- Predictability, a concept related to the notion of accountability, that is, the degree to which a person (the supplier, in commercial domain) meets the expectations of the trustor (i.e., the purchaser) in terms of:
  - reliability and
  - consistence of behavior

Which impacts trust more? Propensity vs. Trustee C/C's?

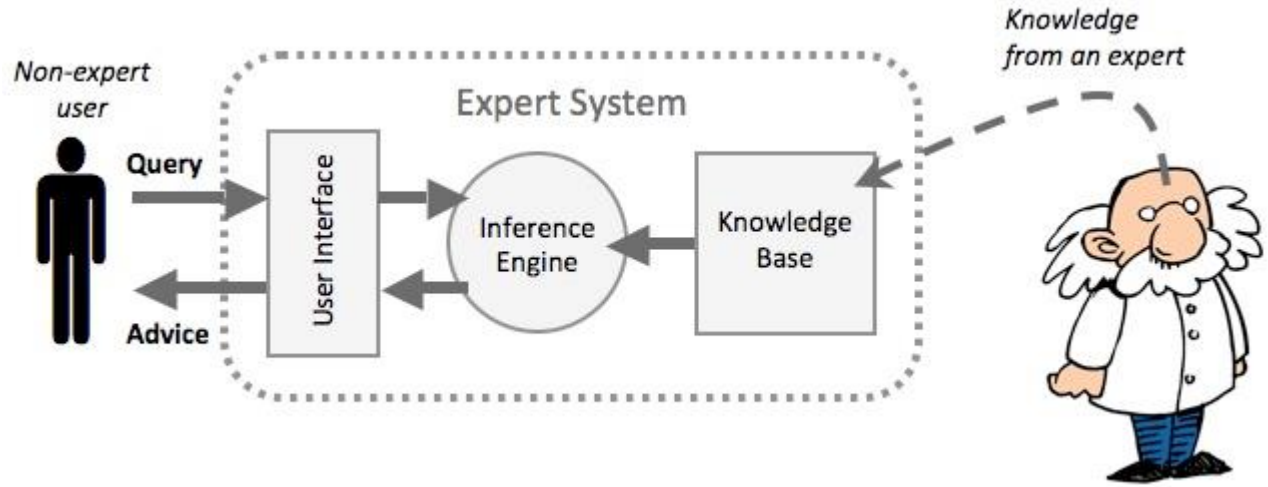
Propensity of Trust

High impact if no info is available on the **INTEGRITY, BENEVOLENCE, & ABILITY** of the Trustee.

No impact if these info are available.

ICT Intermediary Systems

Expert system, Trust Analysis and Management Platform (TAMP), Trust Service Broker (TSB) …etc.



Trustee Available Info

INTEGRITY

The intrinsic moral norms of a trustee to guard his actions with (e.g. sincerity, discretion, honesty)

BENEVOLENCE

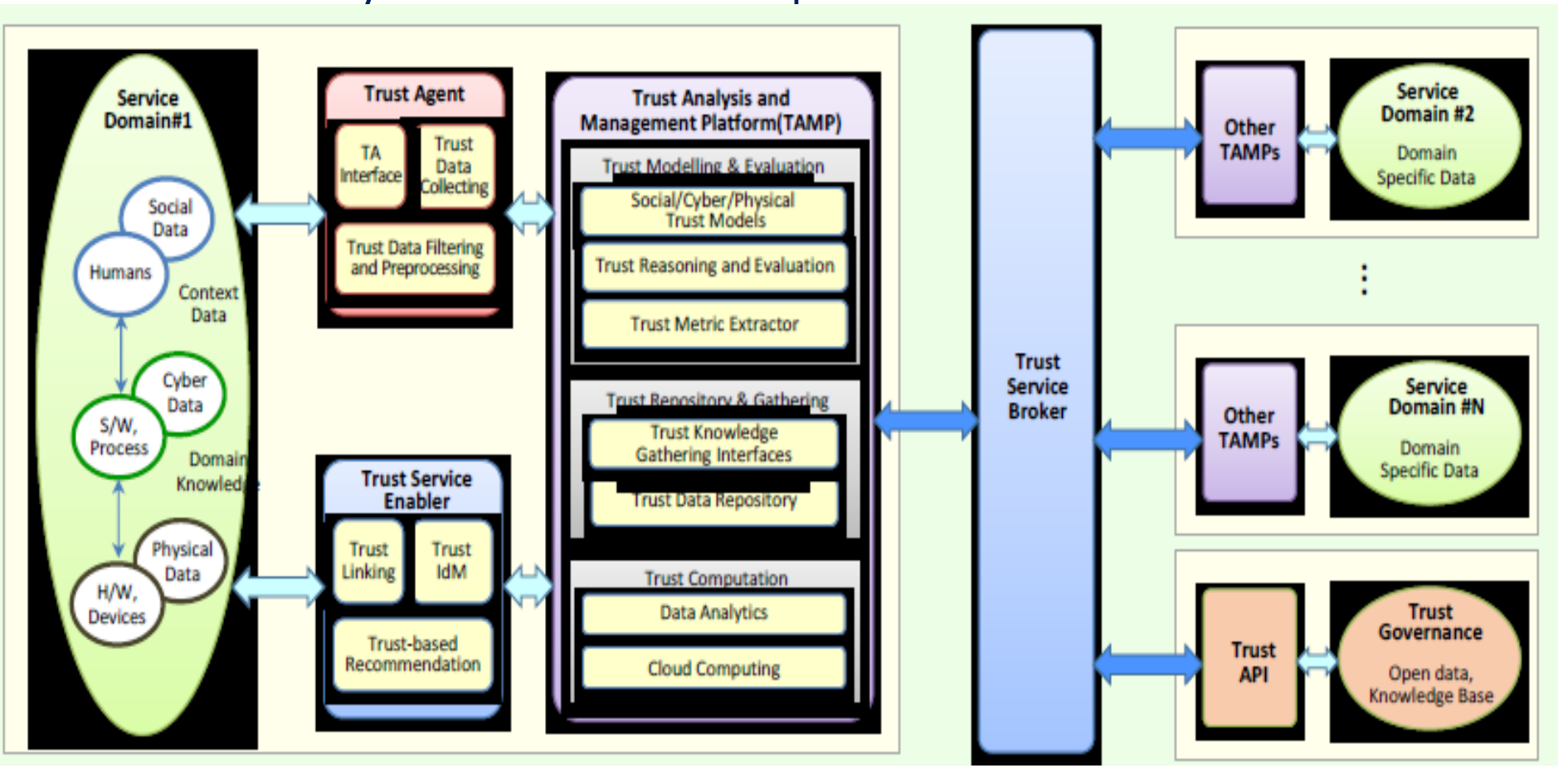
The perceived level of courtesy and positive attitude

ABILITY

Capability of a trustee (based on knowledge, competence, and skills) to perform tasks within a specific domain

Conclusion so far.. Lesson #2

- Trustworthy ICT is an end to end process..



An architectural framework for trust provisioning for ICT infrastructure (ITU-T CG-Trust TR on Trust provisioning for future ICT infrastructures and services)

Conclusion so far.. Lesson #2

- Trustworthy ICT is an end to end process..

Masking the C/C's of the Trustee (i.e. **INTEGRITY, BENEVOLENCE, ABILITY + PREDICTABILITY)** will cause trust to be only affected by the **Propensity of Trust !!!**

Content

- Complexity of Trust
- The Concept of Trust
- Theoretical Framework of Trust
- How big is the risk? And how real is it?
- Relationship to Privacy
- Recommendations and Trustworthy ICT Generic Requirement

So are threats real?

Cars. A leading car manufacturer recalled > 1 million vehicles after demonstrated proof-of-concept attack to take control of the vehicle remotely.

Smart home devices. Millions of homes are vulnerable to cyberattacks. A leading research company unit found multiple vulnerabilities in 50 commercially available devices, including a 'smart' door lock that could be opened remotely online without a password.

Medical devices. Deadly vulnerabilities are found in dozens of devices such as insulin pumps, x-ray systems, CT-scanners, medical refrigerators, and implantable defibrillators.

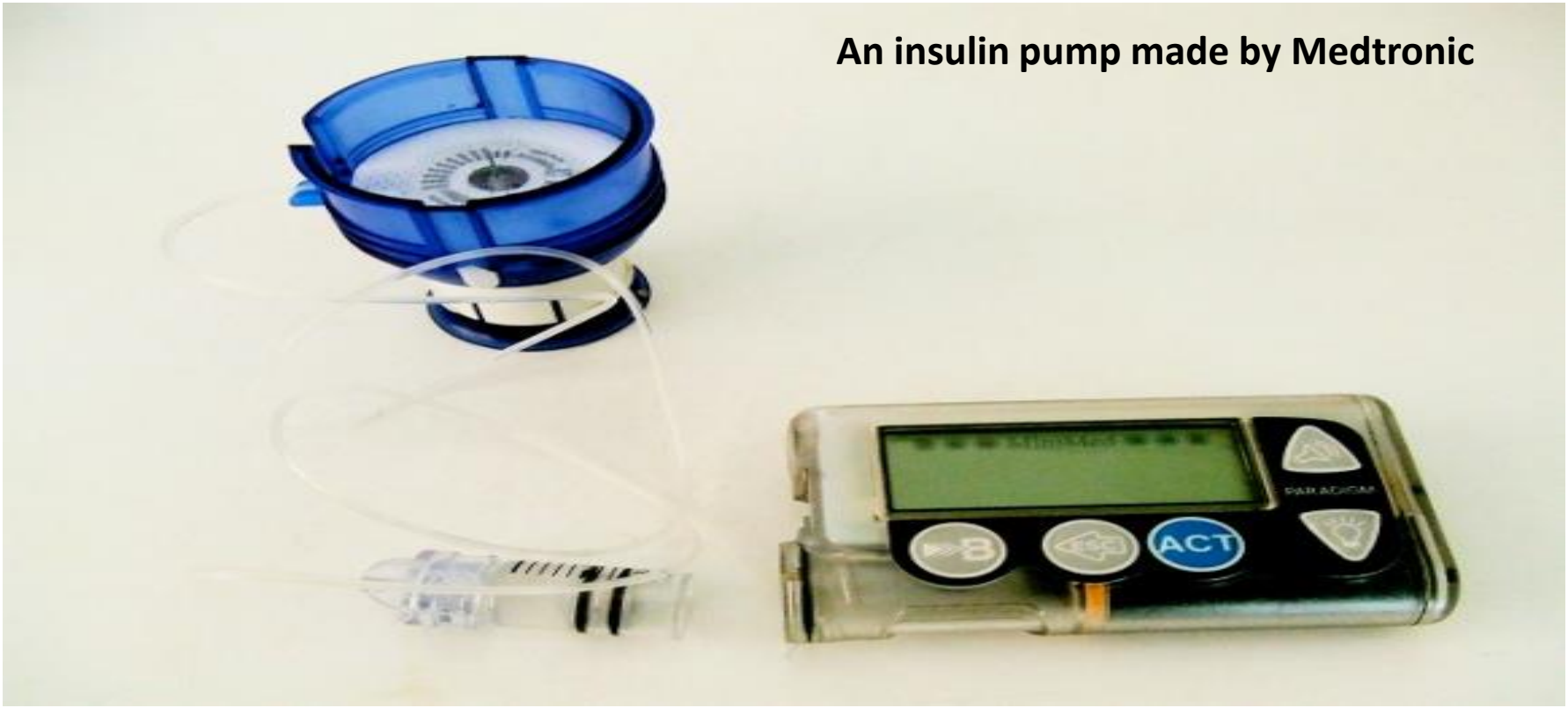
Smart TVs. Hundreds of millions of Internet-connected TVs are potentially vulnerable to click fraud, botnets, data theft, and ransomware, according to Symantec research.

IoT Botnet. 25000 CCTV cameras hacked to form a massive botnet that can blow large websites off the Internet by launching Distributed Denial-of-service (DDoS) attacks.

Hacking Humans !!

Sources: Hackernews, Symantec, Kaspersky

They are real alright!



A security researcher has devised an attack that hijacks nearby insulin pumps, enabling him to secretly deliver fatal doses to diabetic patients who rely on them.

Sources: Hackernews, Symantec, Kaspersky

Dr. Mark Weiser, “father of ubiquitous computing” said..

“The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.”

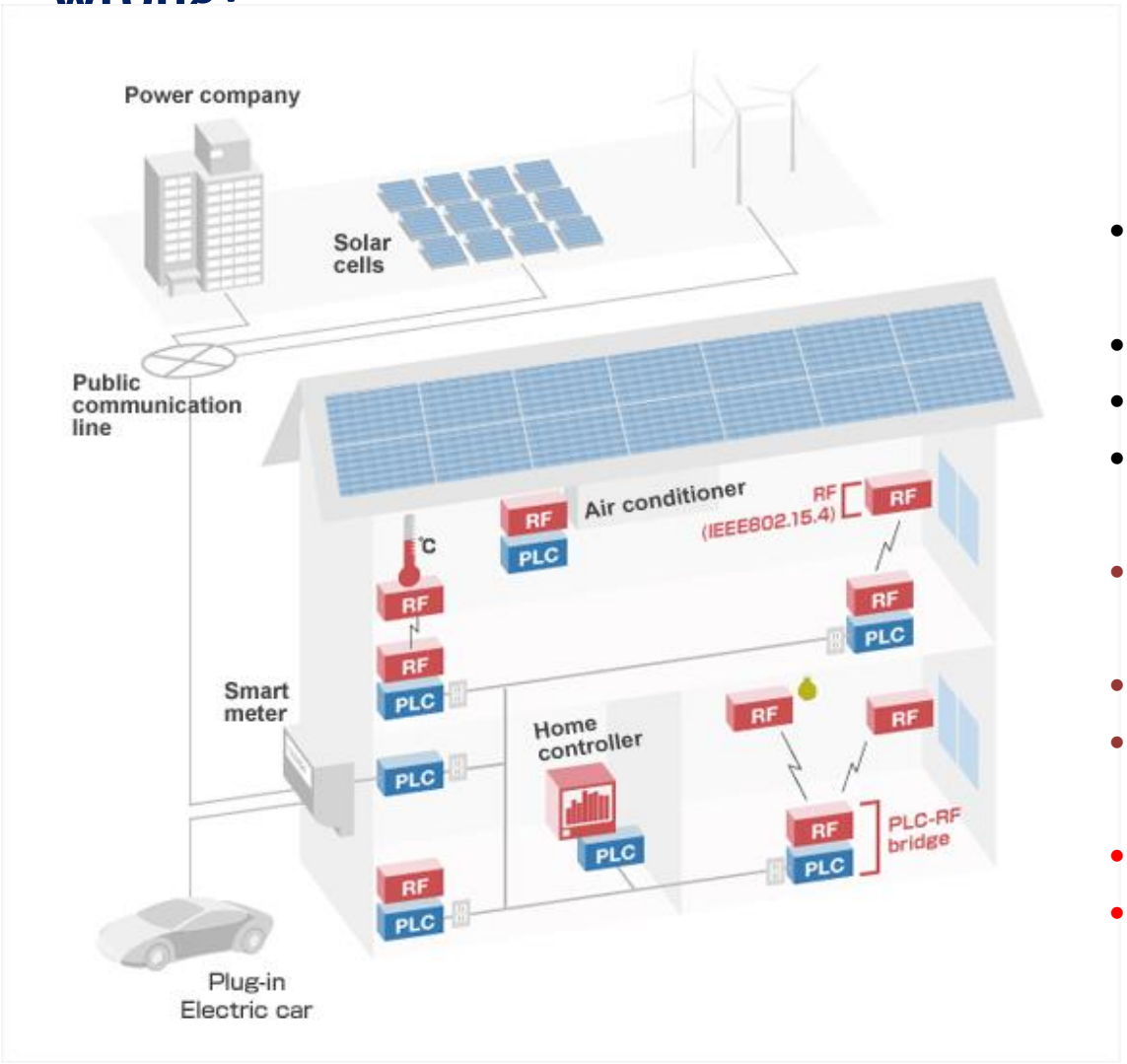
Risk Scenarios for some specific use cases

- Smart Home
- Medical Devices
- Industrial Control Systems

Impact is assessed according to the degree of damage:

- Medium Severity →e.g. User inconvenience, limited financial loss …etc.
- High Severity → e.g. High financial loss, privacy breaches ...etc.
- Critical Severity → e.g. Significant financial loss, health hazards …etc.

In a typical smart home application, what could possibly go wrong?



Medium Severity

High Severity

Critical Severity

- **Denial of communication service attack**
- **Power cut**
- **Air conditioning tampering**
- **Unauthorized 3rd party activity monitoring**
- **Hacking into sensitive usage data (home controllers or meters)**
- **Altering metering data**
- **Spoofing identity of home owner (purchases, contracts ...etc.**
- **Theft**
- **Safety and life threatening incidents (tampering with gas lines & possibility of electric shocks)**

The Anthem case study!

- In 2015, Anthem announced: personal data of about 80 million customers & employees had been compromised
- Anthem is the second largest U.S. health insurer
- Largest ever disclosed attack by a health care company
- Breach did not expose financial information
- Hackers gained access to names, birth dates, Social Security numbers, street addresses, email addresses and employment information.

How?

- ❖ Attacker-owned infrastructure
- ❖ Zero-day exploits
- ❖ Custom developed malware

Three variants are named:
1) **Hurix,** 2) **Sakurel, and** 3) **Mivast**
detected as Trojan.Sakurel — Backdoor.Mivast

Source: Symantec

In a typical Health Application, what could possibly go wrong?

- Consumer Health Monitoring Products
- Wearable external medical devices like insulin pumps
- Internally embedded and implanted devices

Medium Severity

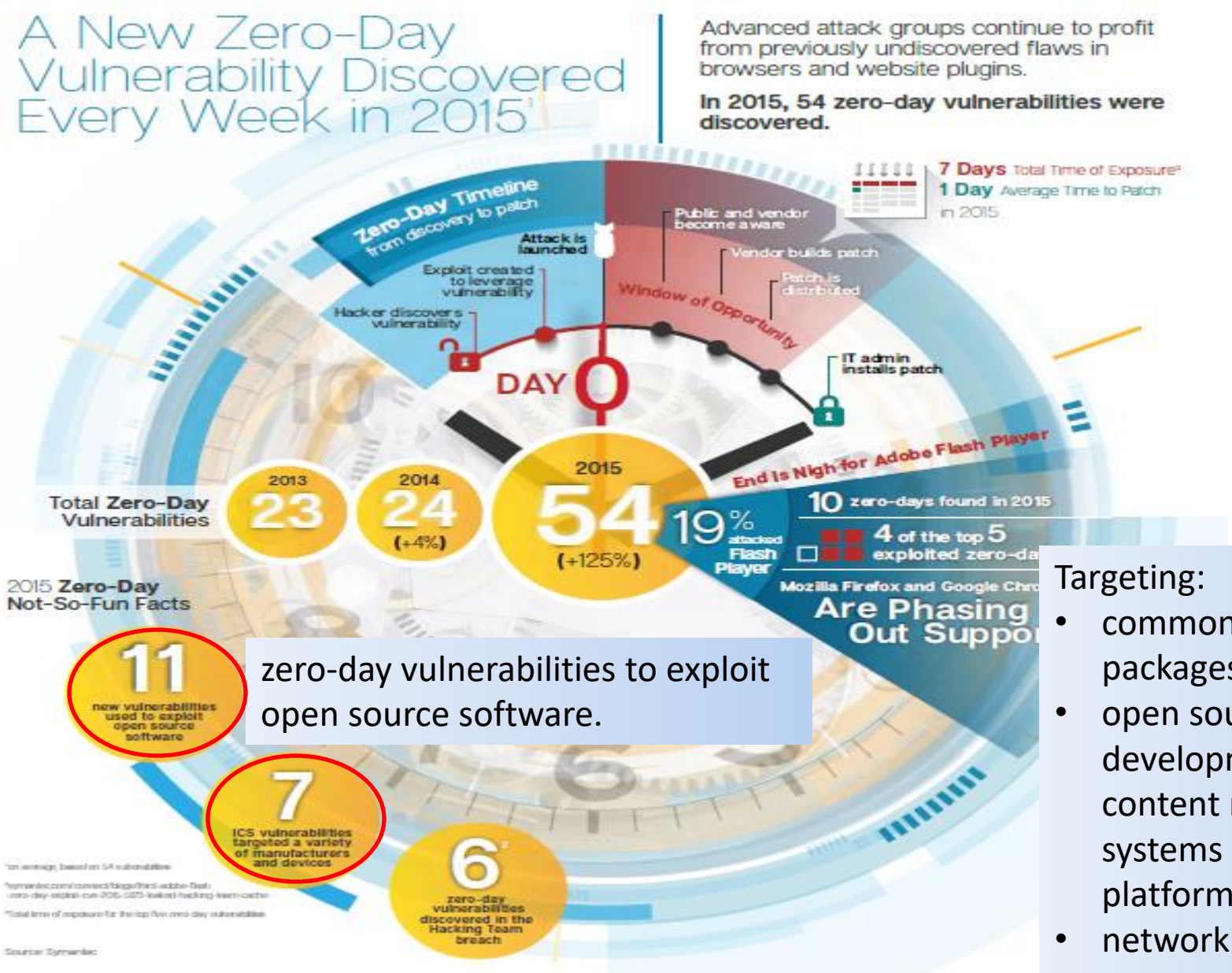
High Severity

Critical Severity

- **Denial of communication service attack (they usually communicate via Bluetooth or proprietary tech.)**
- **Accidental Failure**
- **Patient privacy compromise**
- **Intentional disruption**

According to the Identity Theft Resource Center, 44 percent of all registered data breaches in 2013 targeted medical companies.

Source: Meg Whitman, "10 Big Tech Trends in Healthcare," HP Matter, January 7, 2015, https://www.linkedin.com/pulse/10-big-tech-trends-healthcare-meg-whitman



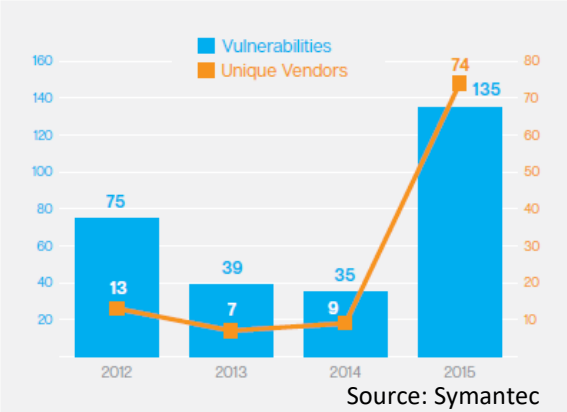
zero-day vulnerabilities to exploit open source software.

Targeting:

- common libraries and packages
- open source web development tools, like content management systems &e-commerce platforms
- networking protocols

7 vulnerabilities in Industrial Control Systems (ICS)

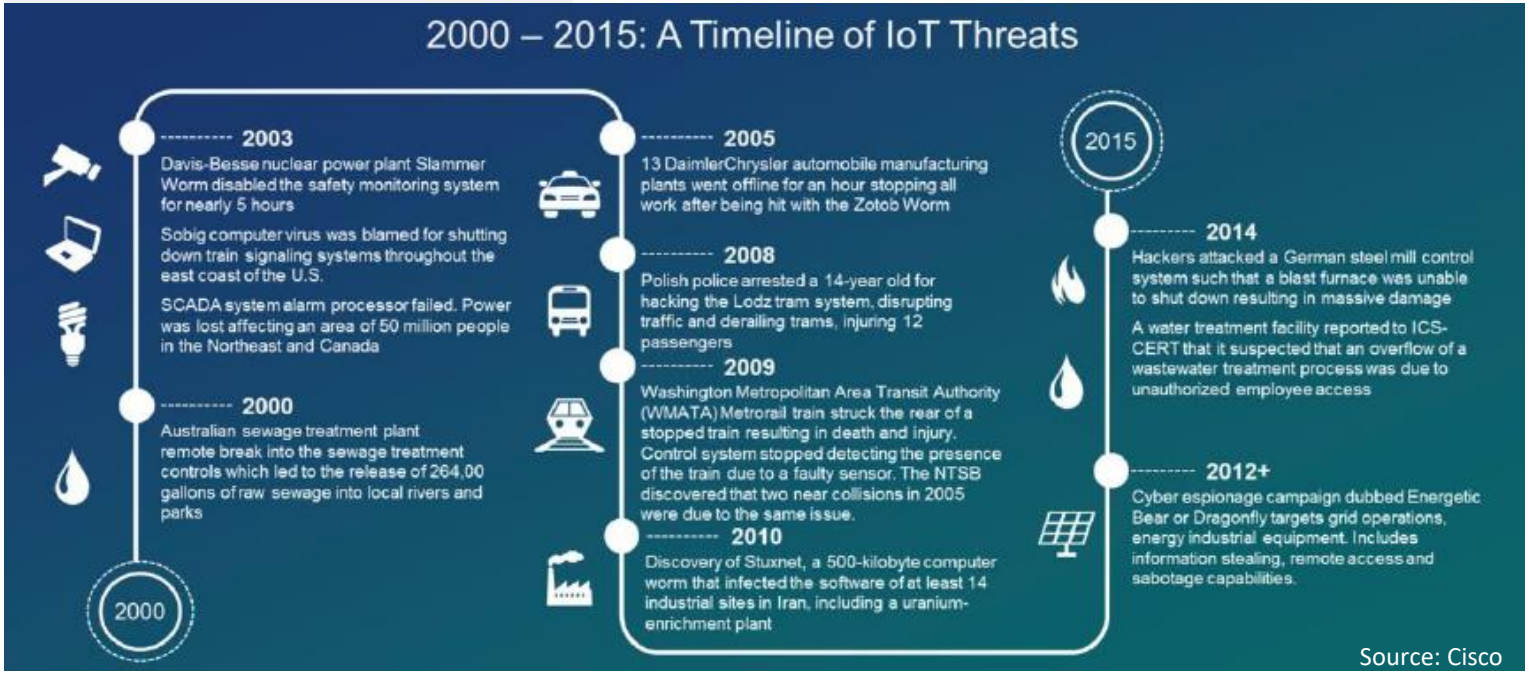
Industrial Control Systems (ICS) .. What could possibly go wrong..



Source: Symantec

Everything?

- Equipment..
- Insecure Process
- No traditional ICT interfaces for which the security companies are used to secure..



Source: Cisco

Industrial Control Systems (ICS) .. What could possibly go wrong..

- Many areas of industrial production and utility services are routinely connected to the Internet for remote monitoring and control
- Many organizations standardize their platforms by using commercial off-the-shelf (COTS) products, such as Windows or Linux
- Windows and Linux are subject to vulnerabilities
- ICS management systems connected with enterprise networks can increase the potential exposure to threats more typically associated with these operating systems

Conclusion so far.. Lesson #3

Risks are real

Content

- Complexity of Trust
- The Concept of Trust
- Theoretical Framework of Trust
- How big is the risk? And how real is it?
- Relationship to Privacy
- Recommendations and Trustworthy ICT Generic Requirement

The Privacy Headache.. The Privacy Right ..

Trust is far more important (1) !

- In the rush to monetize customer data, companies risk diminishing trust users have in their products & services
- Trust have more value than customer data
- Big Data and Social Network Analytics are important tools to create value for the industry..
- But..
- Users are becoming more aware of the implications of using these technologies on their personal privacy

Trust is far more important (2) !

- The end user is now asking on:
  - privacy
  - Who controls their data,
  - How is their data used

- What happens if the industry:
  - Put people before analytics
  - Enabled privacy by default
  - Gave user control, and
  - Were transparent about Data (how it is stored, manipulated, accessed, and who uses it, to do what?)

Personally Identifiable Information (PII)

Personally Identifiable Information (PII): Any information

a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains;

b) from which identification or contact information of an individual person can be derived; or

c) that is or can be linked to a natural person directly or indirectly.

Source: ITU Rec. ITU-T X.1252 (04/2010)

Includes:

- an individual's name, gender, age, address, photo, and occupation
- personal data and records held by financial, health and medical, utilities, telecom, and other government agencies
- email, phone numbers, Skype/messaging accounts, and contacts list
- mobile location, travel, and other addresses
- shopping purchases, phone bill, and credit card
- Internet and social networking activity, and their call history
- personal preferences and interests
- friends' and families' preferences and interests

Source: Ovum

Privacy could be compromised intentionally or unintentionally..

Top 10 Sectors Breached by Number of Incidents

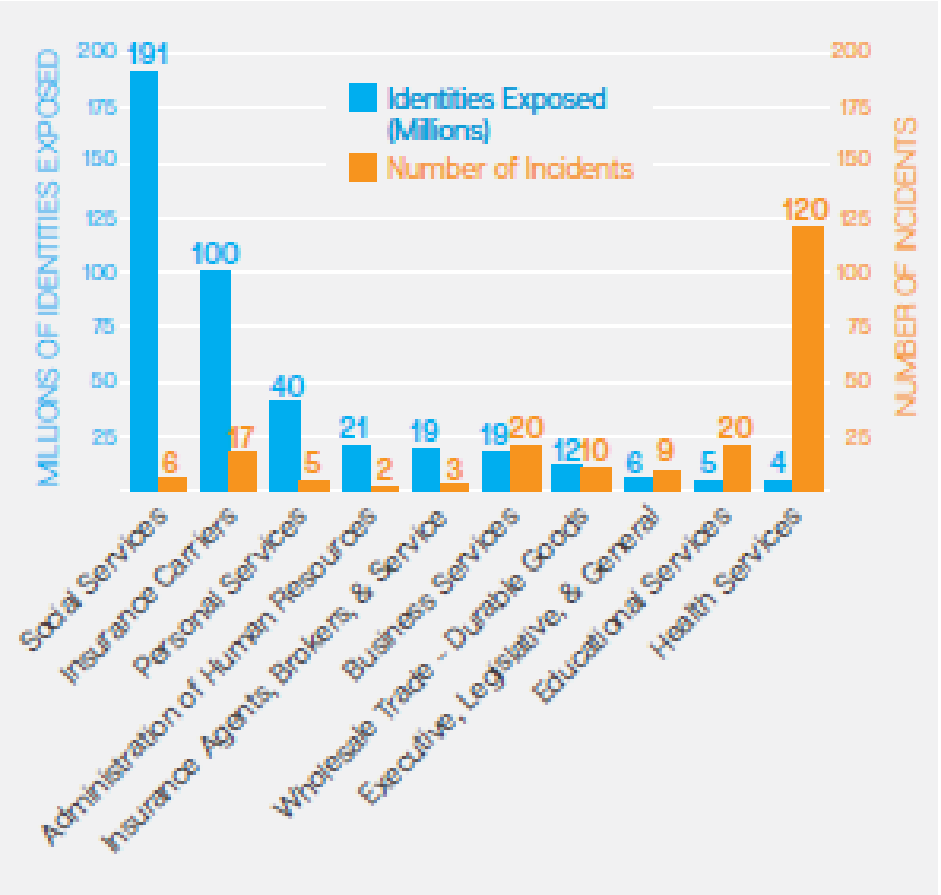
	Sector	Number of Incidents	% of Incidents
1	Services	200	65.6%
2	Finance, Insurance, & Real Estate	33	10.8%
3	Retail Trade	30	9.8%
4	Public Administration	17	5.6%
5	Wholesale Trade	11	3.6%
6	Manufacturing	7	2.3%
7	Transportation & Public Utilities	6	2.0%
8	Construction	1	<1%

Top 10 Sectors Breached by Number of Identities Exposed

	Sector	Number of Incidents	% of Incidents
1	Services	259,893,565	60.6%
2	Finance, Insurance, & Real Estate	120,124,214	28.0%
3	Public Administration	27,857,169	6.5%
4	Wholesale Trade	11,787,795	2.7%
5	Retail Trade	5,823,654	1.4%
6	Manufacturing	3,169,627	<1%
7	Transportation & Public Utilities	156,959	<1%
8	Construction	3,700	<1%

39 percent of all breaches reported by a major security player in 2015 were attributed to the healthcare industry.. What does that tell you?

- Privacy should be protected
- Regulations might be needed to ensure that data are adequately safely stored, used, and processed conditioned by the user's consent



Conclusion so far.. Lesson #3

Trust have more value than customer data

Content

- Complexity of Trust
- The Concept of Trust
- Theoretical Framework of Trust
- How big is the risk? And how real is it?
- Relationship to Privacy
- Recommendations and Trustworthy ICT Generic Requirement

So now comes the big question.. Now that we know the risks and its magnitude.. What is required?

- Trustworthy systems should:
  - mitigate risks against the compromise of authenticity, confidentiality, integrity, non-repudiation, and availability of devices, systems, applications, protocols, platforms, and services,
  - prevent unlawful traceability, profiling, and unlawful processing of big data systems, applications, platforms, and services,
  - publish data policies,
  - be audited by trusted third parties.

Risk assessment models + Trustee C/C's are essential to be merged in order to realize Trustworthy ICT.

Impact Vector	Information Attack Source	System Environment Attack Source	Physical Attack Source	Attack Target
I-S	Yes	No	No	System (S)
S-I	No	Yes	No	Information (I)
I-S-I	Yes	No	No	Information (I) using (S)
I-S-P	Yes	No	No	Physical using (S)
P-S-I	No	No	Yes	Physical (P)
P-S-P	No	No	Yes	Physical using (S)
S-P	No	Yes	No	Physical (P)
P-S	No	No	Yes	System (S)

Information Space (I) System and Device Environment (S) Physical Space (P)

Source: Adapted from Draft Recommendation ITU-T Y.IoT-sec-safety

Impact Vectors Examples (1)

Impact vector	Description	Examples
I-S	Cyberattack targeting the system from within its informational environment	Denial of service attack Confidential information stealing
S-I	Expoliting software bugs or concealed system features harming security of environment without any influence. May be treated as system informational safety.	Improperly implemented or infected with malware system harming other
I-S-I	Cyberattack targeting the informational environment of the system by exploiting improperly implemented system features	Cross-site scripting (XSS) Distributed denial of service using botnet
I-S-P	Cyberattack targeting the physical environment of the cyber-physical system and intended to cause physical damage or harm physical aspects of system execution.	Stuxnet APT on Natanz nuclear facility An attack on an unnamed German steel mill facility Proof-of-concept attack on car security

Impact Vectors Examples (2)

Impact vector	Description	Examples
P-S-I	Actions posing problems for information security aspects by purely physical means.	Destroying hardware, cable breakage Physical tampering of video surveillance systems by placing a picture in front of a camera
P-S-P	Physical hazards that are usually capable of harming the environment or people	Sabotage, negligence Faulty treatment
S-P	Exploiting software bugs or functions that may affect important factors in the physical environment. May be treated as system functional safety.	System functions implemented without or with insufficient consideration of safety requirements
P-S	Physical hazards that are usually capable of harming the system or its components	Disregard of operating instructions Faulty treatment

Takeaway Messages..

Privacy and data protection

M2M, IoT, Future Network applications, services, infrastructure record a wide variety of PII

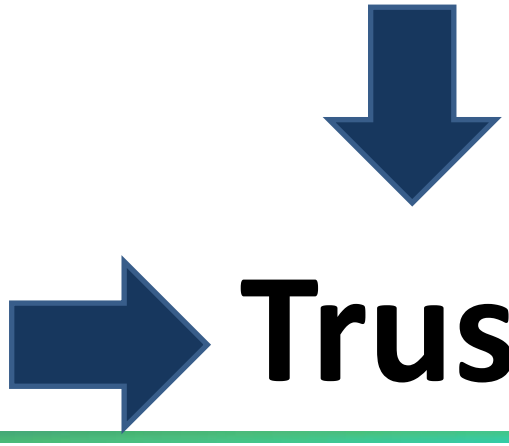
End user is often unaware of the amount and detail of his PII is being gathered and/or shared when they use a service, a system, a device, or an application

Enforce regulations on :

- How information should be stored, processed, and distributed
- Measures to delete customers data (the right to be forgotten)
- Easily identifiable contact details if customers had privacy concerns
- …

Network security and resilience

New measures to detect vulnerabilities and potential threats.
Threat Impact Vectors are needed to analyze and detect the potential sources of breaches, the potential targets, and the potential operating environment of these breaches..
why?
To develop sound security measures.



Thank you

Dr. Ramy Ahmed Fathy, PhD

ramy.ahmed@ieee.org