



Technology Trends, Risks and Responses - An ENISA Perspective

Steve Purser | Head of COD
Bratislava | 15 November 2016

European Union Agency for Network and Information Security

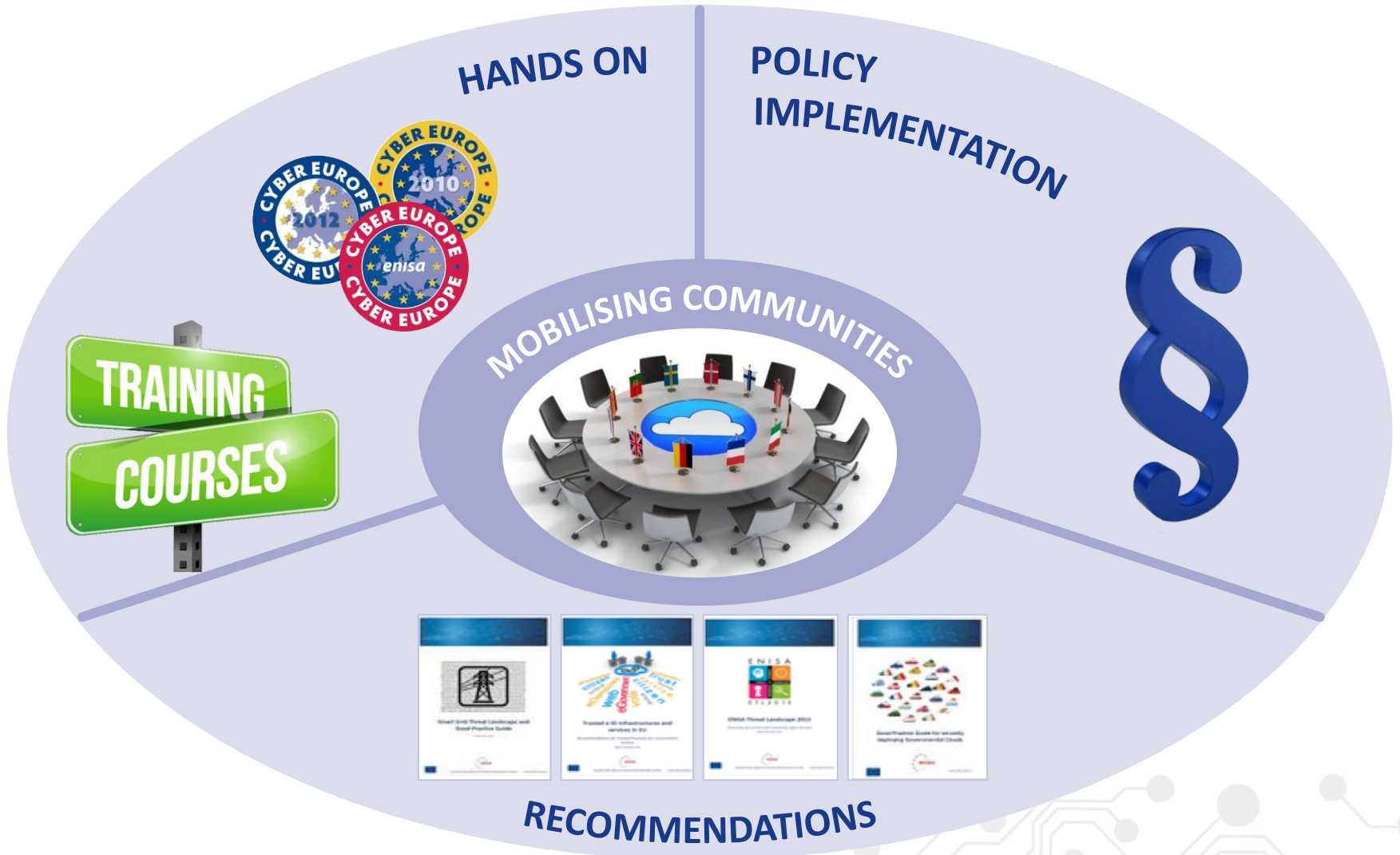


Agenda



- 1** About ENISA
- 2** Technology trends & cybersecurity risks
- 3** The ENISA Threat Landscape
- 4** SMART Environments
- 5** Securing the IoT
- 6** Future challenges

Positioning ENISA activities









Agenda



- 1** About ENISA
- 2** Technology trends & Economic Factors
- 3** The ENISA Threat Landscape
- 4** SMART Environments
- 5** Securing the IoT
- 6** Future challenges

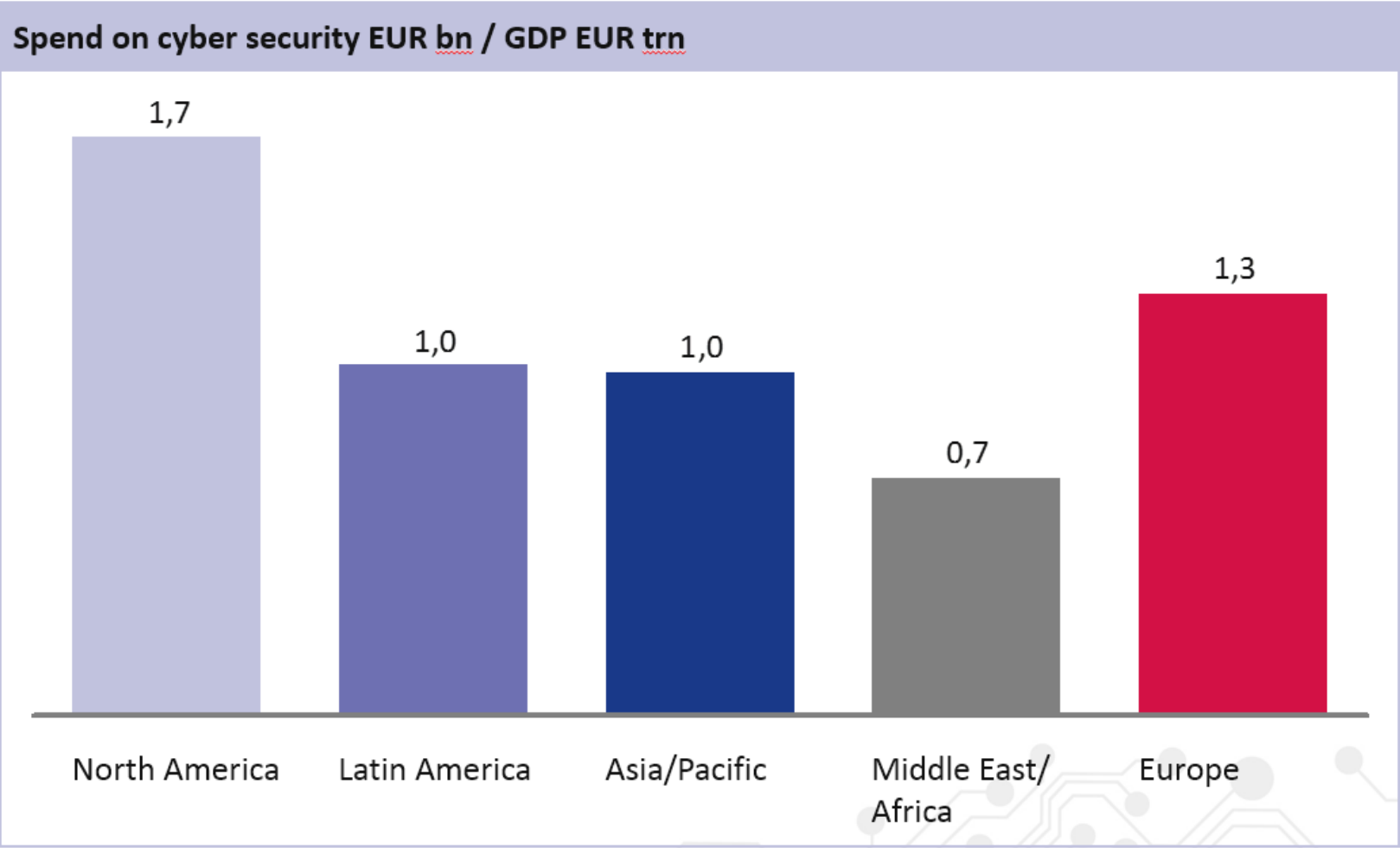
Technology trends



	Description of technology	Growth trend
 Big data	<ul style="list-style-type: none"> Ability to run complex calculations on big amounts of data in a meaningful time frame 	<ul style="list-style-type: none"> Global 33% CAGR 2011-2015
 Sensors and actuators	<ul style="list-style-type: none"> Introduction of cheap sensors and actuators to collect huge amounts of data 	<ul style="list-style-type: none"> Potential \$4-11 economic impact estimated in 2025
 Cloud computing	<ul style="list-style-type: none"> Hosting of software on centralized servers with high-speed access through the Internet 	<ul style="list-style-type: none"> Global 27% CAGR in public cloud services revenues
 Mobile technology	<ul style="list-style-type: none"> Massive increase of mobile computing power, storage, and bandwidth 	<ul style="list-style-type: none"> Global 27% CAGR in mobile-to-mobile communications revenues
 Natural user interfaces	<ul style="list-style-type: none"> Creation of new kinds of interfaces that allow for more intuitive handling of IT systems 	<ul style="list-style-type: none"> 30% reduction in page visits per click
 Computation, storage, and networks	<ul style="list-style-type: none"> Possibility to store large amounts of data and transfer the data with high bandwidth between computers 	<ul style="list-style-type: none"> Global 15% CAGR in enterprise storage market

SOURCE: Gartner, MGI, Team analysis, CAGR = compound annual growth rate

The European Cyber Security market is a significantly lower proportion of GDP than North America, and higher than other regions

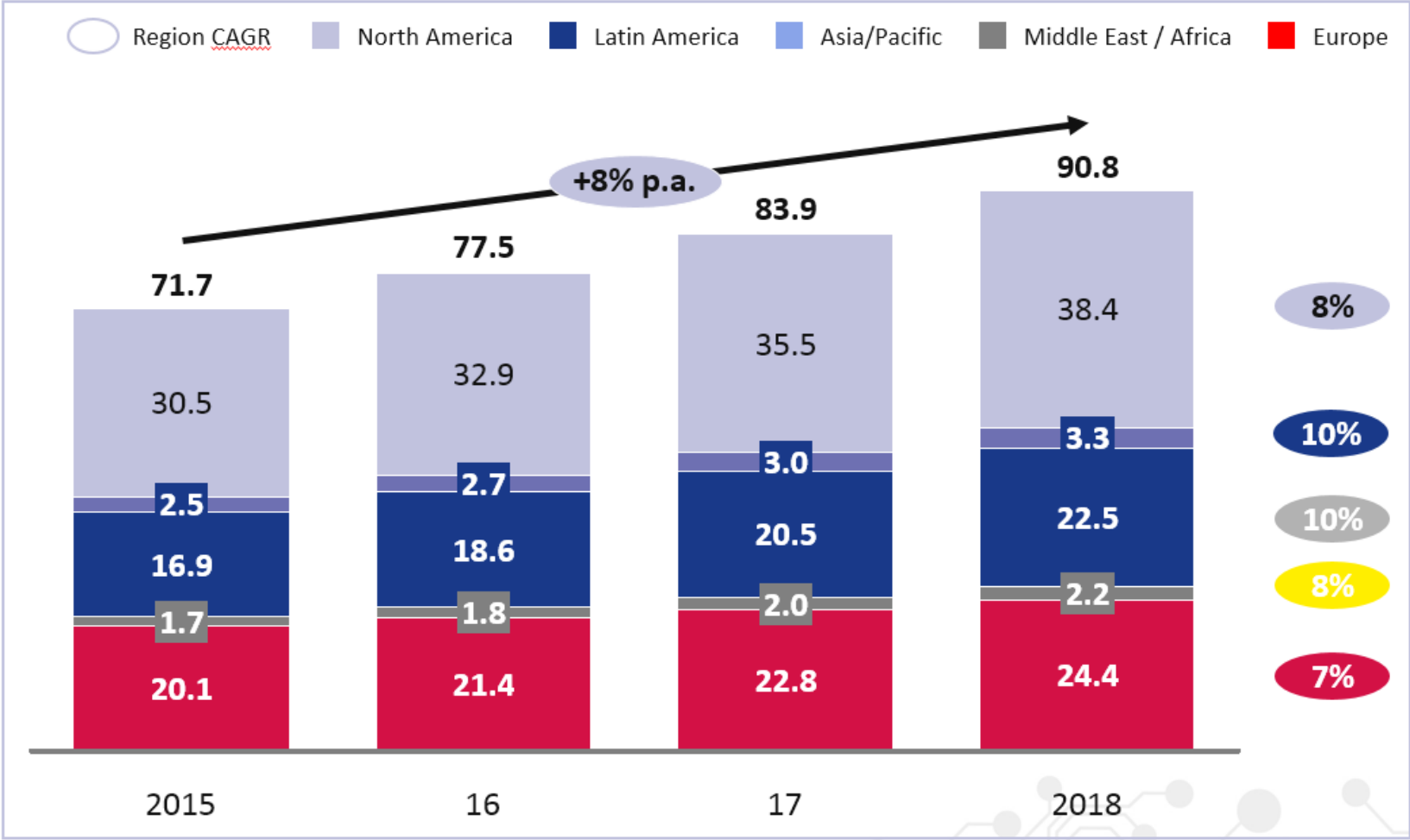


SOURCE: Cyber-security market size in Europe – Gartner 2014, IMF 2013

The European Cyber Security market is growing more slowly than all other regions

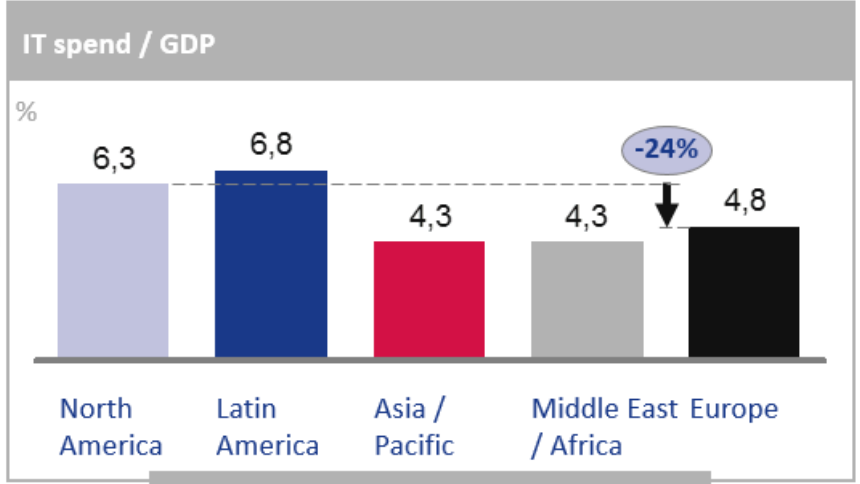
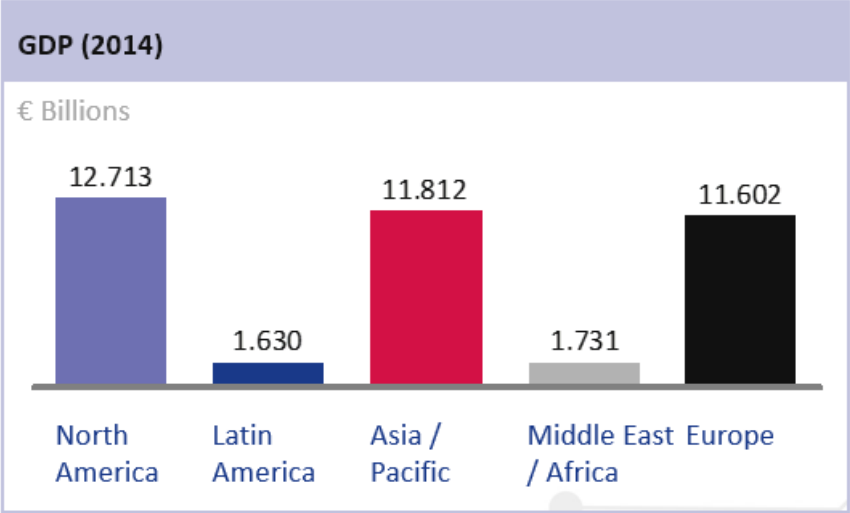
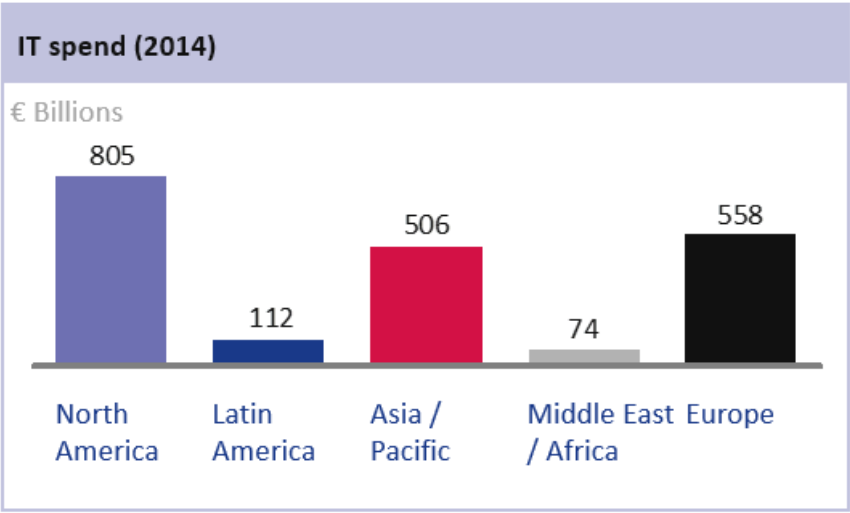


EUR Billion



SOURCE: Cyber-security market size in Europe – Gartner 2014

Europe spends a lower proportion of GDP on IT, indicating lower adoption of technology



Europe spends 24% less on IT as a proportion of GDP than North America

SOURCE: Cyber-security market size in Europe – Gartner 2014, HIS - World Industry Service

The cost of incidents – measured by ENISA



- Findings:
 - **Finance, ICT and Energy** sectors have the **highest incident costs**
 - The **most common cyber attack types for financial sector and ICTs** appear to be **DoS/DDoS and malicious insiders**,
 - The *most costly attacks* are considered to be insider threats, followed by DDoS and web based attacks
 - In terms of country losses, the figures demonstrate up to 1.6% GDP in some EU countries. Other studies mention figures like 425,000 to 20 million euro per company per year
- Note: findings based on a systematic review of publicly available studies published by ENISA in August 2016.

Agenda



- 1** About ENISA
- 2** Technology trends & cybersecurity risks
- 3** The ENISA Threat Landscape
- 4** SMART Environments
- 5** Securing the IoT
- 6** Future challenges

The ENISA Threat Landscape



The ENISA Threat Landscape provides an overview of threats and current and emerging trends.

It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends.

Over 380 recent reports from a variety of resources have been analysed.



THE TOP THREATS

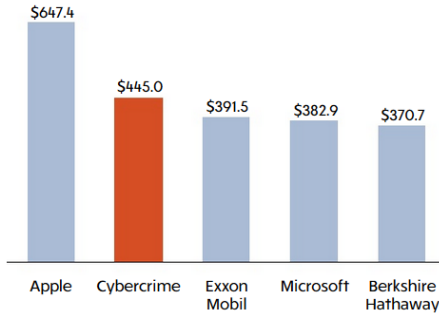


Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans		1. Malware		
2. Web-based attacks		2. Web based attacks		
3. Web application /Injection attacks		3. Web application attacks		
4. Botnets		4. Botnets		
5. Denial of service		5. Denial of service		
6. Spam		6. Physical damage/theft/loss		
7. Phishing		7. Insider threat (malicious, accidental)		
8. Exploit kits		8. Phishing		
9. Data breaches		9. Spam		
10. Physical damage/theft /loss		10. Exploit kits		

ENISA Threat Landscape 2016: Preview



Market Capitalization (\$, Billions)



Source: Bloomberg, cybercrime cost from Allianz Cyber Risk Guide

2016: Year of Cyber-Crime Monetization

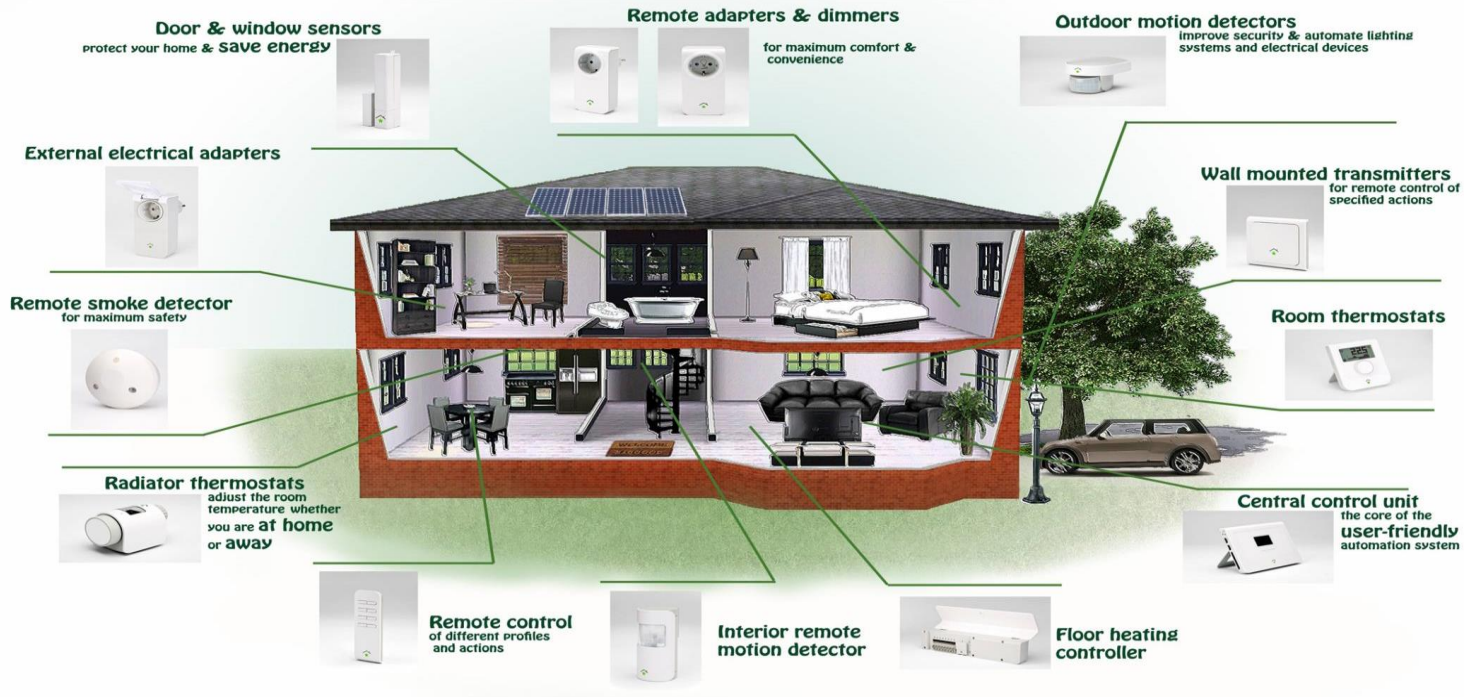
- Cyber-Crime Capitalisation in 2016 would reach the level of the second most valuable US company
- Ransomware families are 175% up and average ransom is 100%. up (600-700\$)
- Data Breaches are as of today 20% over last year
- The first 1Tbps DDoS attack has happened. It has shown impact DDoS-attacks may have (internet service latencies)
- Cyberspace is a recognised battlefield. This creates a new centre of gravity for the whole cyber-security community
- In 2016 we have seen the impact and scale of striking power of **taking over IoT objects.**

Agenda



- 1** About ENISA
- 2** Technology trends & cybersecurity risks
- 3** The ENISA Threat Landscape
- 4** **SMART Environments**
- 5** Securing the IoT
- 6** Future challenges

Smart houses



NOT SO SMART HOME

[f Like](#) 50 [f Share](#) 50 [t Tweet](#) 39 [g+1](#) 5 [in Share](#) 0

Researcher Says It Only Takes Minutes To Hack Most Smart Home Security Devices

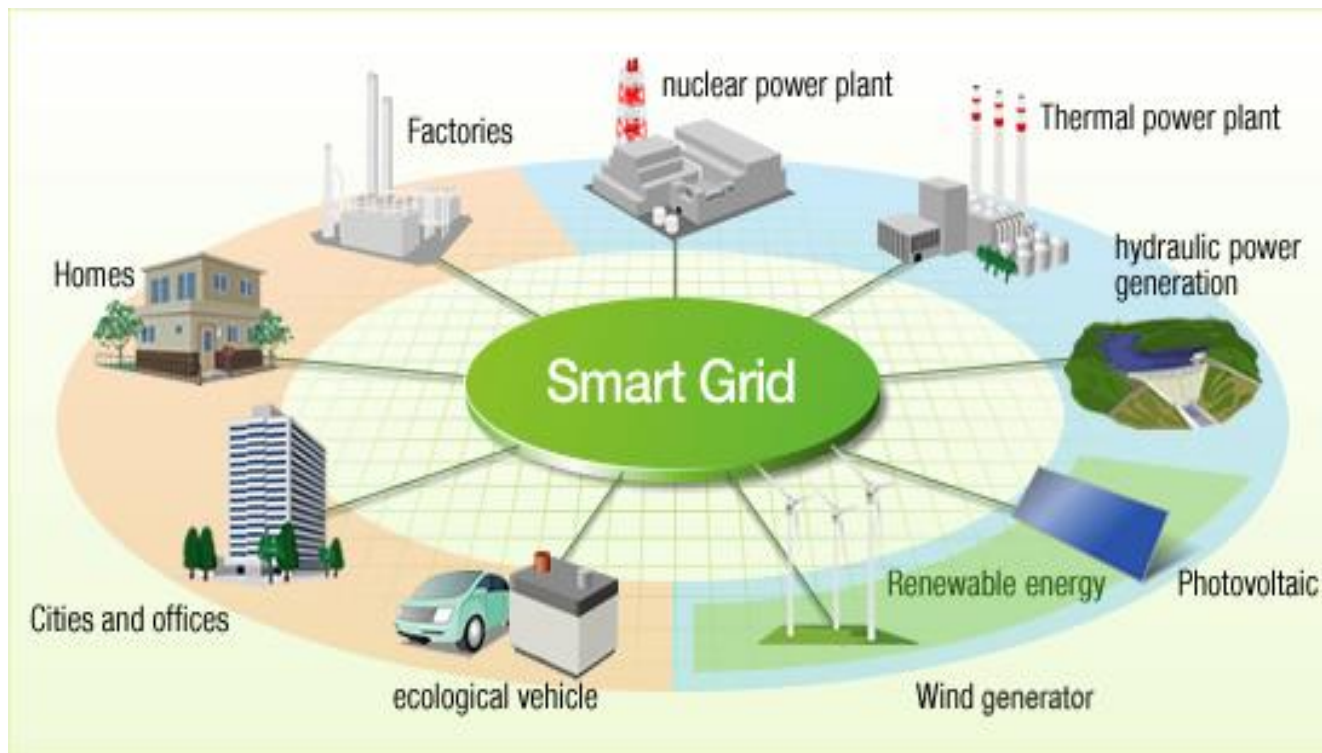
By Ashlee Kiehl February 11, 2015

SMART Homes - Findings



- **Not all smart homes are created equally.** There are multiple design pathways that lead to functional smart homes, ranging between localised and integrated home-automation systems. These pathways have their own security and privacy peculiarities, but also have shared issues and vulnerabilities.
- **Smart homes will have significant privacy and data protection impacts.** The increased number of interlinked sensors and activity logs present and active in the smart home will be a source of close, granular and intimate data on the activities and behaviour of inhabitants and visitors.
- **Several economic factors may lead to poor security** in smart home devices. Companies involved in the smart home market include home appliance companies, small start-up companies, and even crowd-funded efforts. These groups are likely to lack security expertise, security budgets and access to security research networks and communities.
- **The interests of different asset owners in the smart home are not necessarily aligned** and may even be in conflict. This creates a complex environment for security activity.
- Just as in many other areas of ICT, **applying basic information security would significantly increase overall security** in the smart home domain.

Smart grids



From: <http://cleantechnica.com/2014/02/19/global-smart-grid-investment-grows-china-leads-us-falls-behind>

BloombergBusiness News Markets Insights Video

Hackers Find Open Back Door to Power Grid With Renewables

SMART Grids Certification (2014)



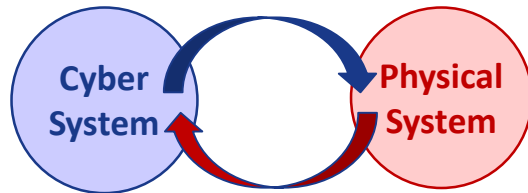
- Harmonised EU smart grid security certification practices.
 - More harmonised and coordinated EU smart grid certification practices will act as an umbrella and should contain building blocks national schemes need to have.
- National implementation of specific smart grid use cases based on a chain of trust.
 - Each Member State should be able to map its preferred national standard/scheme to the EU platform and refer to this national standard for details.
- Oversight.
 - It is recommended to create a EU steering committee with oversight competences on smart grid certification, the definition of pan European security requirements' and the development of national schemes

Agenda



- 1** About ENISA
- 2** Technology trends & cybersecurity risks
- 3** The ENISA Threat Landscape
- 4** SMART Environments
- 5** **Securing the IoT**
- 6** Future challenges

IoT Challenges & Risks



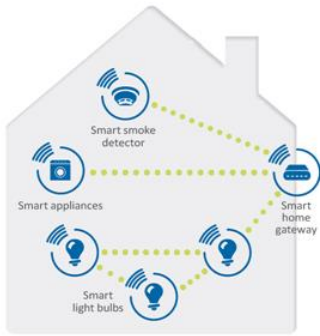
Current challenges of IoT

- Capacity-limited devices
- Data exchange with other devices and remote services
- No regulation on data ownership
- Interaction with the physical life (*cyber-physical systems*)
- Economic limitations

Threats and risks of IoT devices and services

- Threats are diverse and evolve rapidly
- Several IoT manufacturers are not expert in security
- Data collection and processing may be unclear to users
- Impact on citizens' health, safety and privacy

ENISA and IoT security



ENISA studies Security and Privacy for:

- Devices
- Data exchange (including network infrastructure)
- Local and remote services (*e.g.* Cloud, etc.)

ENISA develops expertise to secure IoT

- Evaluation of threats
- Promotion of security and privacy good practices
- Stakeholders engagement
- Awareness raising
- Community expert groups
- Liaison with policy makers



Domains of activities



Smart Cities



**SCADA
and Industry 4.0**

In 2015:

- Smart Cities and Intelligent Public Transport
- Smart Homes

In 2016:

- Smart Cars
- eHealth and Smart Hospitals
- Smart Airports
- Industry 4.0

Target audience:

- Operators and end-users
- Manufacturers, developers and solution vendors
- Policy makers and supervision bodies (DPAs, NRAs, etc.)
- But also: academy, standardisation bodies...



Smart Homes



eHealth

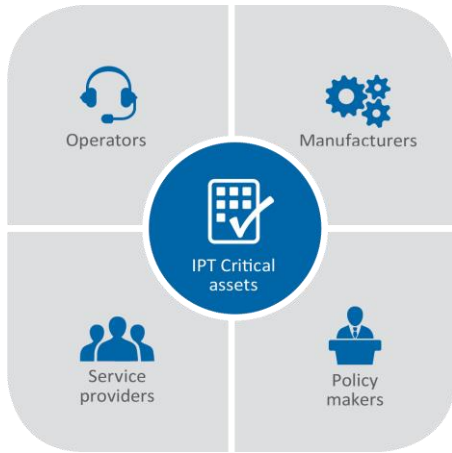


**Intelligent
Transportation Systems**

Recommendations to secure IoT



ENISA recommendations:



- Promote collaboration on cyber security across Europe
- Develop awareness raising on IoT threats and risks
- Establish a governance model for cyber security
- Integrate security in business processes (trade-off risk/investment)
- Define security requirements to ensure “security for safety”

Agenda



- 1** About ENISA

- 2** Technology trends & cybersecurity risks

- 3** The ENISA Threat Landscape

- 4** SMART Environments

- 5** Securing the IoT

- 6** Future challenges

Some Future Challenges



- Training and maintaining adequate skill sets
- Leveraging cybersecurity as a market enabler.
- Achieving agile support processes such as standardisation and certification
- Building cybersecurity into the industrial process.
- Aligning cybersecurity with safety considerations.
- Implementing strong privacy and data protection principles in a business-friendly manner.



Thank you

 PO Box 1309, 710 01 Heraklion, Greece

 Tel: +30 28 14 40 9710

 info@enisa.europa.eu

 www.enisa.europa.eu

