Internet resilience

Udo Helmbrecht

Executive Director, ENISA

Simulation techniques, Munich, 26/01/2015

Agenda

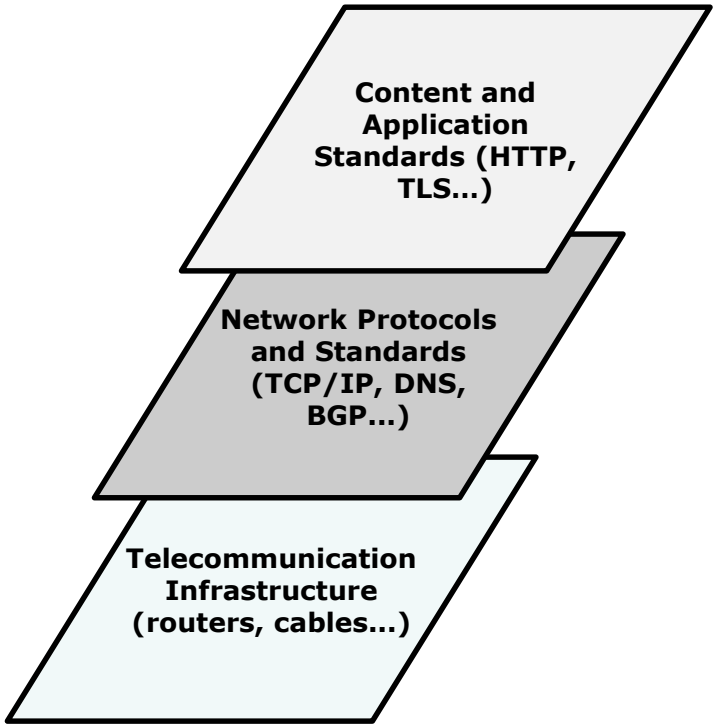
- Today's Challenges
  - Current Internet Infrastructure Threats
  - ENISA Activities
- Cloud Security Challenges
  - Risk Assessment in the cloud
  - Governmental Clouds
  - Cloud Security Certification
- Big Data- New topic, new challenges

IT Security:

- Confidentiallity
- Integrity
- Availibility

Today's challenges

There is increasing reliance on communication networks



There is an emerging threat environment hampering the availability, integrity and confidentiality of networks based on:

- Infrastructure vulnerabilities
- Interdependencies
- Privacy concerns
- Growing threat landscape

ENISA activities

Latest released **study**:

- **Threat Landscape and Good Practice Guide for Internet Infrastructure** to give and overview of emerging threats and good practices to face large scale incidents such as amplification attacks and route hijacks

Flash Notes in case of large scale incidents:

- 2013 DNS amplification attacks, 2014 NTP reflection attacks, Heartbleed, Shellshock…

Community engagement:

- INFRASEC - **Internet infrastructure security and resilience reference group**: experts from Internet operations to discuss current threats and future challenges to secure European networks.

ENISA Threat Landscape Report

Figure 4 – Threat taxonomy of the Internet infrastructure (levels 1 and 2 - see Annex C for the expanded mind map)

http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl

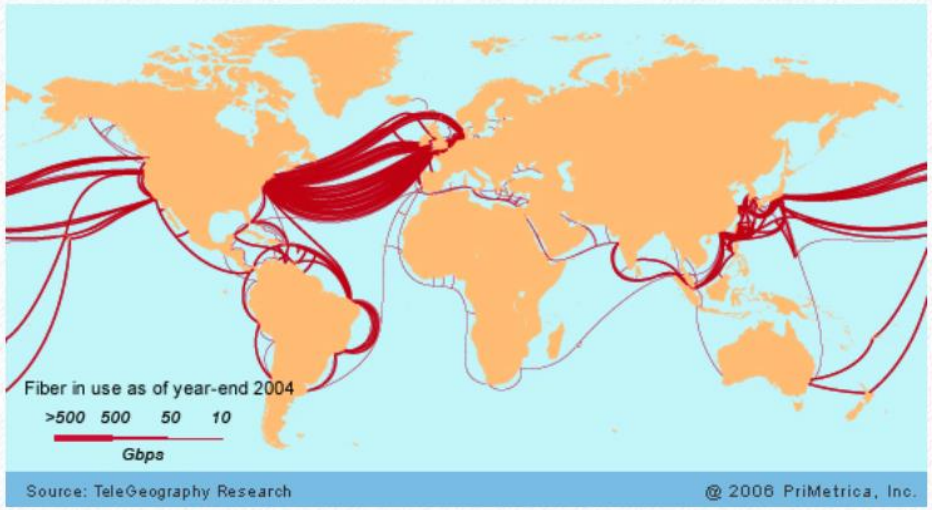
Current Internet infrastructure threats

Threat groups	Threat types	Trends
Routing Threats	Nefarious Activity/Abuse	Increasing
	Eavesdropping/Interception/Hijacking	Increasing
DNS Threats	Nefarious Activity/Abuse	Decreasing
Denial of Service	Nefarious Activity/Abuse	Increasing
Generic Threats	Physical attack	N/A
	Damage/Loss	Increasing
	Failures/Malfunctions	Increasing
	Nefarious activity/Abuse	Increasing
	Eavesdropping/Interception/Hijacking	Increasing

https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl

Saboteurs Cut Undersea Internet Cable Near Egypt

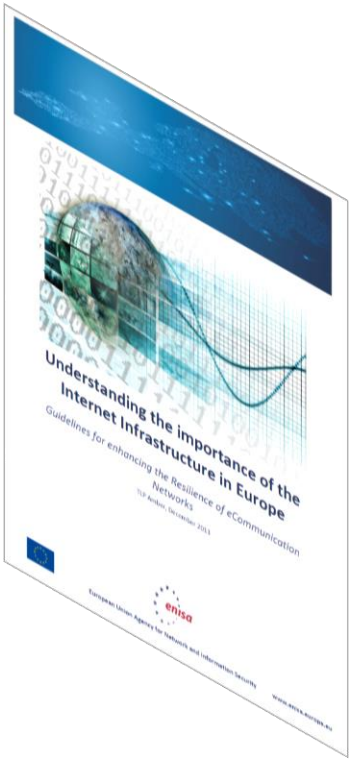
IDG News Service – Egypt said it has arrested three men suspected of slicing a crucial undersea Internet cable on Wednesday, causing widespread problems from Kenya to Pakistan.



The South East Asia-Middle East-West Europe 4 (SEA-ME-WE 4) cable runs 12,500 miles from France to Singapore, with branches connecting telecommunication companies in Malaysia, Thailand, Bangladesh, India, Sri Lanka, Pakistan, United Arab Emirates, Saudi Arabia, Egypt, Italy, Tunisia and Algeria.

28.08.2013 http://earthfirstjournal.org/newswire/2013/03/28/saboteurs-cut-undersea-internet-cable-near-egypt/

The Internet Infrastrucure



Assets

Physical	Logical
• Landing stations • Undersea cables • Buried cables • Colocations sites • Internet Exchange points • Generic provider infrastructure	• IP address • IP blocks of addresses • Autonomous System Numbers (ASNs). • Routes • DNS infrastructure • Uniform resource locators (URLs)

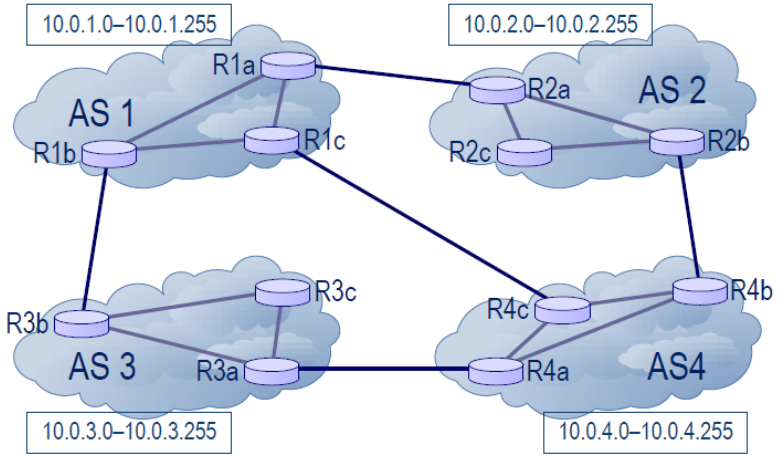
Routing Tables

Routing Table for R1a:

10.0.1.0–10.0.1.255	*Local*	
10.0.2.0–10.0.2.255	Path: 2	via R2a
10.0.3.0–10.0.3.255	Path: 3	via R1b
10.0.4.0–10.0.4.255	Path: 4	via R1c
	or Path: 2, 4	via R2a

Routing Table for R1b:

10.0.1.0–10.0.1.255	Local	
10.0.2.0–10.0.2.255	Path: 2	via R1a
10.0.3.0–10.0.3.255	Path: 3	via R3b
10.0.4.0–10.0.4.255	Path: 4	via R1c
	or Path: 3, 4	via R3b



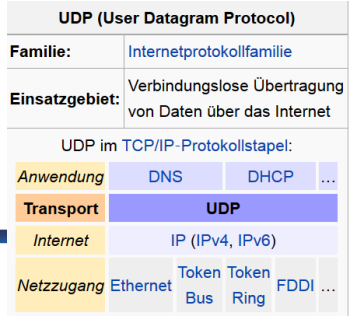
Routing Table for R2a:

10.0.1.0–10.0.1.255	Path: 1	via R1a
10.0.2.0–10.0.2.255	*Local*	
10.0.3.0–10.0.3.255	Path: 1, 3	via R1a
	or Path: 4, 3	via R2b
10.0.4.0–10.0.4.255	Path: 4	via R2b
	or Path: 1, 4	via R1a

Routing Table for R2b:

10.0.1.0–10.0.1.255	Path: 1	via R2a
	or Path: 4, 1	via R4b
10.0.2.0–10.0.2.255	*Local*	
10.0.3.0–10.0.3.255	Path: 4, 3	via R4b
	or Path: 1, 3	via R2a
10.0.4.0–10.0.4.255	Path: 4	via R4b

Example of a Flash-Note



Large scale UDP attacks: the 2014 trend and how to face it

Flash Note 02, 24th February 2014

"Recent news show the increase of large scale attacks1 exploiting specific vulnerabilities of the Internet core protocols. In the latest cases, the Network Time Protocol (NTP), which allows synchronizing devices to the coordinated universal time (UTC), has been misused. Specifically, in December 2013, a vulnerability in this UDP protocol became mainstream and started to be exploited for large scale reflection attacks leading to a dramatic increase of the size of denial of services. Luckily, network providers can already put in place a series of known countermeasures to mitigate these threats, as ENISA underlined also for amplification attacks in April 2013.

…

"

Securing European networks

- Evaluate your current level of security by understanding the assets covered (and not covered) by existing security measures.
- Evaluate the application of adapted good practices in a focused manner.
- Cooperate with the network community to exchange on threats and promote the application of good practices as mitigation measures.
- Report on implementations of good practices, assets covered and gaps found.
- Words matter: Ensure the right use of terms and definitions.

Securing European networks

- Use proper risk assessment methods to understand vulnerable assets in your Internet infrastructure and prioritise your protection actions.
- Build an information and communication technology security awareness and training program.
- Commit third-party vendors to apply security measures.
- Stay current on any update

All ENISA Internet Infrastructure studies can be found here
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x

ISPs and IXPs

LIBERTY GLOBAL

orange™

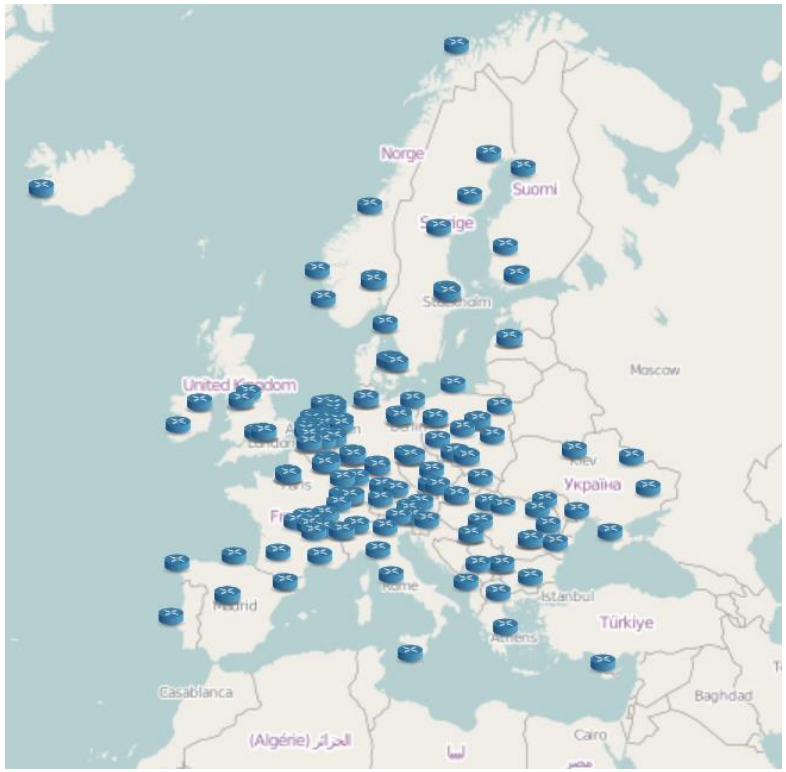
TELE2

Telefónica

telenor

Telia

vodafone



ISPs in Europe (examples)

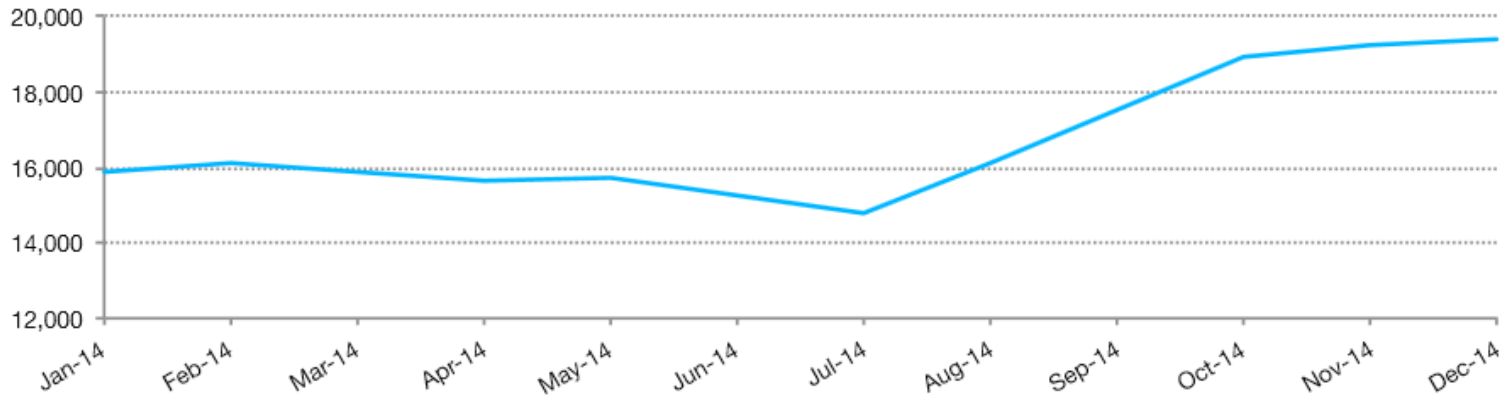
http://www.internetanbieter.eu

IXPs in Europe

http://www.ixptoolkit.org

The importance of IXPs in Europe

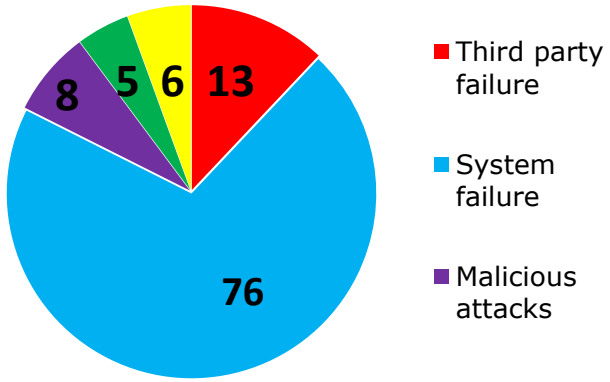
- Largest IXPs carry on a daily basis traffic volumes in the petabyte range, similar to what some of the largest global ISPs reportedly handle
- End-to-end flow of traffic in today's Internet has to include as key component the IXPs and the networks that peer at those IXPs
- Critical for understanding how content is distributed in today's Internet and how the different parties (e.g., content providers, CDNs, ISPs) are adapting



Total aggregated traffic growth in the Euro-IX region (in Gbps) in 2014 - Source: Euro-IX IXPs Traffic Statistics 2014 summary

RegTelCo-Incident-Reporting by ENISA

- 1st report in 2012 (Art 13a TelCo Reg., on 2011's incidents - 51)
- 2nd report in 2013 (on 2012's incidents);
- 79 incidents from 18 countries,
- 9 countries without incidents,
- 1 country without implementation (9 in 2011)
- Most incidents affect mobile comms (50% of incidents, 1.8 Mn/incident)
  - Natural disaster, power cuts outages affected 2.8 Mn/incident
- Ca 40% impact on emergency number 112



https://www.enisa.europa.eu/media/press-releases/new-major-incidents-in-2012-report-by-eu-cyber-security-agency-enisa

Cloud Security Challenges

- Software security vulnerabilities
- Network attacks
- Social engineering attacks
- Insecure interfaces and APIs
- Vendor lock in and Cloud migration
- Compliance issues
- International data privacy laws
- Critical Clouds

Risk Assessment in the Cloud

Famous 2009 Guide

First Ever Risk Assessment For Cloud computing

Updated in 2012

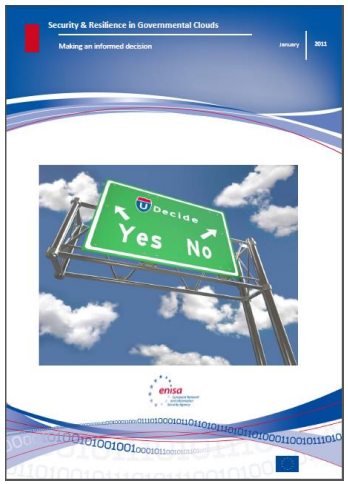
New updated catalogue

Security Guide for SMEs – 2015

Risk Assessment focused on SME opportunities – together with an online tool

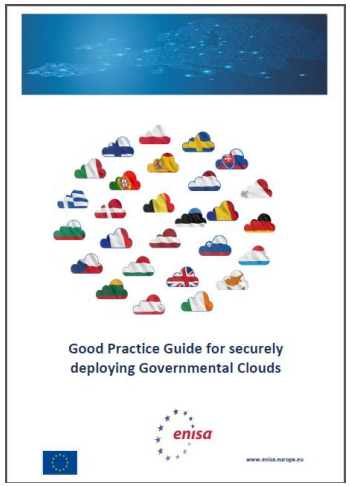
All ENISA Cloud studies can be found here: https://resilience.enisa.europa.eu/cloud-security-and-resilience

Governmental Clouds (1/2)



2010: Guide on security and resilience for Governmental Clouds

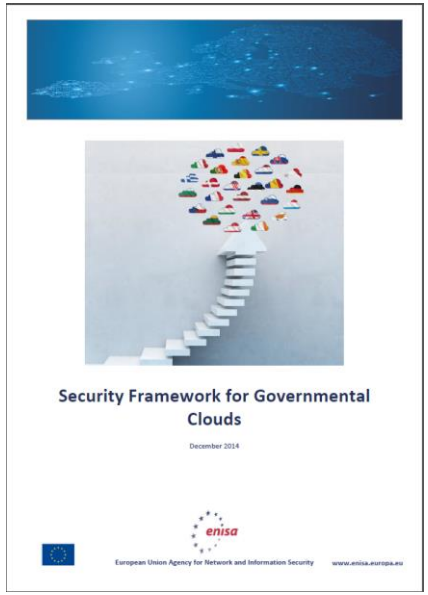
- Presentation of the security benefits and drawbacks for the public sector to go in the cloud
- First steps need to be done towards taking the decision to go cloud



2013: Good practice guide on how to securely deploy Governmental Clouds

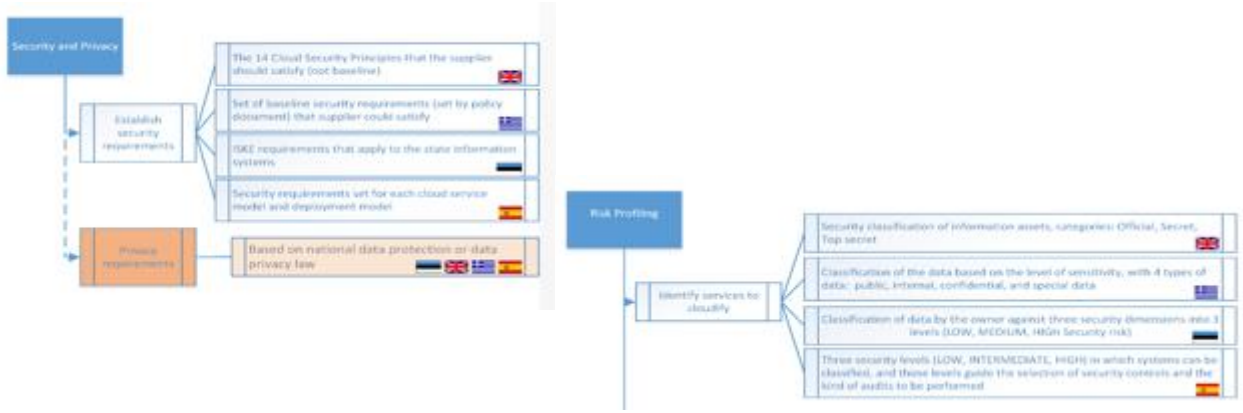
- Definition of a governmental cloud (in a mature market)
- State of cloud computing adoption in the EU public sector
- Case studies of different approaches in adopting a cloud solution

Governmental Clouds (2/2)

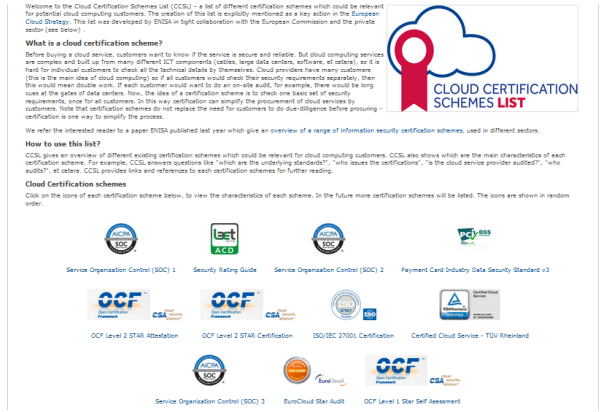


2014: Security framework for Governmental Clouds

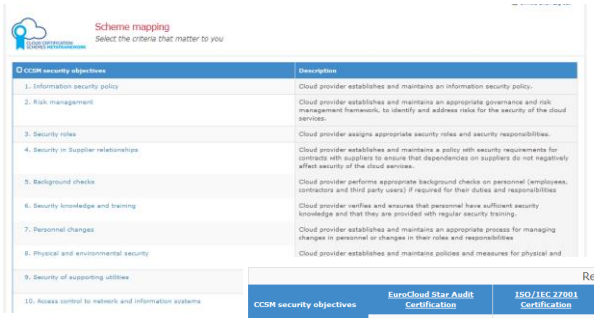
- Security (and privacy) framework for the public administration to adopt cloud computing
- The framework presents the **4 phases (PDCA) – 9 activity domains- 16 security** steps from the pre-procurement phase till the finalization of the contract and exit, covering all the roles and the tasks with use cases.

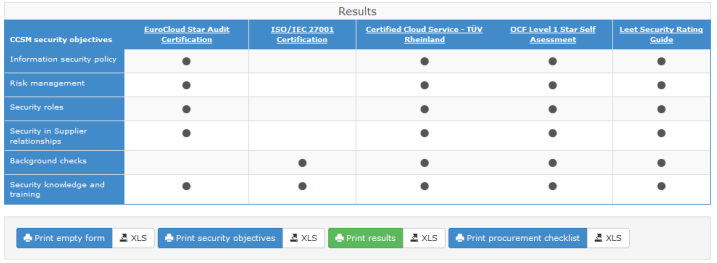


ENISA and Cloud Certification



- Cloud Certification Schemes List (CCSL): List of existing certification schemes
  - 12 Certification schemes included
  - Powered by ENISA, supported by the EC and the Cloud Selected Industry Group (C-SIG)
- Cloud Certification Schemes Meta-framework (CCSM): Meta-framework based on existing certification schemes
  - Mapping detailed ICT security requirements of the public sector in the EU (11 countries and more will come)
  - MATRIX will results to be used for procurement





Visit: https://resilience.enisa.europa.eu/cloud-computing-certification

Big Data: new topic, new challenges?

Big Data: Collection of data sets so large that its management and use present significant challenges

Security Challenges:

- Infrastructure Security
- Secure data storage and transactional logs
- Continuous monitoring and audit
- Validity and governance
- Data privacy (for mining and analytics)

In 2015 ENISA will study the Security and Resilience of Big Data

Thank you for your attention

For more information visit: http://www.enisa.europa.eu

Follow ENISA: