ENISA/ISACA workshop 11 June, 2013 Berlin Germany

@ ISACA World Congress, "Insights 2013", Estrel Berlin, Sonnenallee 225, Berlin, Germany

ENISA and ISACA® are pleased to offer this unique "invitation only" workshop to address today's Cyber security challenges

Theme: Auditing Security Measures in the Electronic Communications Sector

The 2009 reform of the European legislation for electronic communications introduced Article 13a, which requires electronic communications providers to 1) assess risks, 2) take appropriate security measures to prevent security incidents, 3) and report about security incidents. In most countries this triangle is supervised by the telecom regulator.

Generally speaking, for a regulatory authority, supervising security across a sector of service providers is not easy. One reason is that in most countries the sector consists of hundreds of businesses and they range from very small operators (<1% of the market), to large multinationals (>10% of the market) who may even have infrastructure across borders. This means that risk assessment are different for different providers, and also the security measures in place are very different.

Note that the supervision required by Article 13a is just one example where national authorities are asked to supervise security across a sector. Similar to Article 13a, there is Article 4 of the e-Privacy directive (also part of the 2009 reform) which requires providers to take security measures to prevent personal data breaches. Along the same lines are Article 15 of the proposed directive on eSig/eID providers and Article 14 of the recently proposed cyber security directive, which obliges countries to supervise operators in critical sectors in the same way.

This workshop aims to bring together the expertise and experience of telecom operators, ISPs, auditors, and national regulators. We will focus on the following questions:

- How can providers show supervisors (in a cost-effective way) that appropriate security measures are in place?
- How can providers re-use existing governance frameworks and tools?
- How can government authorities supervise that appropriate security measures are being taken across a sector?
- What is the role of auditing and certification in this, and who should bear the auditing costs and get the detailed audit reports, etc.?

Workshop Details

This complimentary, interactive workshop will focus on the security measures mandated by national and EU legislation, and how government authorities supervise that the providers in the sector take appropriate security measures.

After an initial status update of cyber security legislation and the state-of-play in the telecommunications sector, a series of presentations will be delivered from three different perspectives: the regulatory authority, the service provider and finally the auditor. An open panel discussion will follow where additional ideas and viewpoints will be exchanged among the panelists and invited guests to better understand the issues, applied solutions and areas for stronger collaboration.

Preliminary Agenda

13:00-14:00 Registration and lunch

14:00 – 14:30 Opening Remarks

Dr. Marnix Dekker and Christoffer Karsberg, security experts at ENISA and Dr. Christos K. Dimitriadis, ISACA International Vice President

- Importance of having a framework for security measures. risk assessment and incident reporting
- Security governance in Article 13a & EU cyber security directive

14:30 – 16:00 Featured Presentations

Manuel Pedrosa de Barros, Director, Anacom Portugal
Gensériс Cantournet, Security Vice-President, Cross Processes and Projects, Telecom Italia

A prominent regulatory authority, service provider and auditor will each present their unique perspectives toward:

- Implementing the provision on the notification of security breaches found in Article 13a
- Addressing risks to resilience and security
- Identifying good practices and procedures for collecting and reporting incidents
- Learning from implementations conducted to date and developing consistent enforcement
- Developing a unified scheme for auditing and reporting

16:00 – 16:30 Coffee Break

16:30 – 18:00 Open Panellist and Guest Discussion

Among topics that will be addressed are:

- Enterprise risk assessment: How/can we do national risk assessments? How does this translate to the risk assessments of providers?
- Are current ISO27000 series information security frameworks appropriate? Is a recovery time objective of 2 days acceptable?
- How can/should a regulatory authority implement continuous monitoring, exercises, tests, scans, and incident reporting into a single governance framework for an entire sector?
- Do these frameworks apply to smaller providers? Are maturity models appropriate or are they only used by very large providers?
- What is the effectiveness of preventive audits vs post-incident audits, and what is the role of auditors?
- What can we learn from the telecommunications sector (for example) and use in emerging, unregulated sectors, like cloud computing or social media?

18:00 – Reception and Continued Discussion

Do you want to attend the workshop or do you want further information, please contact Christoffer Karsberg, ENISA: Christoffer.karsberg@enisa.europa.eu