ENISA ISACA Cyber Security Workshop - Highlights

1 Introduction

11 June 2013 ENISA and ISACA held a joint workshop on Auditing Security Measures in the electronic communications sector. The workshop took place in Berlin in conjunction with the ISACA Insights Congress, and the workshop was attended by more than 25 organizations from 15 countries representing supervisory authorities, electronic communications providers and auditors.

The workshop covered Article 13a in the European Union Framework Directive of the Telecom Reform. This article requires electronic communications providers to assess risks, take appropriate security measures to prevent security incidents, and report on security incidents to their national regulator. This triangle of activity is generally supervised by a telecom regulator, which has the challenging task of supervising security across a sector of service providers consisting of hundreds of businesses ranging from very small operators to large multinationals who have infrastructure across borders.

The workshop was divided in two sessions, a presentation session and a panel session with discussions.

The presenters and participants in the panel were:
Terry Trsar, Chief Relations Officer, ISACA, opening and closing remarks
Christos K. Dimitriadis, ISACA International Vice President
Evangelos Ouzounis, Head of Unit, ENISA, moderator
Christoffer Karsberg, Expert in Network and Information Security, ENISA
Manuel Pedrosa de Barros, Director, Anacom Portugal
Gensériс Cantournet, Security Vice-President, Cross Processes and Projects, Telecom Italia
Michael Hofmann, Partner and Head of Information Risk Management; IT Audit, Attestation, Advisory, KPMG Luxembourg

2 Highlights from presentations

The ENISA-ISACA workshop started with a status update of cybersecurity incident reporting legislation in the EU, followed by a series of presentations from three different perspectives: the regulatory authority, the service provider and finally the auditor. The following sections provide the highlights from these presentations.

2.1 Cyber security incident reporting in the EU - ENISA

ENISA gave a presentation on cyber security incident reporting and security measures in the EU. Focus was on Art 13a in the electronic communications framework directive which has logics in common with Art 4 in the ePrivacy Directive, Art 30-32 in the proposed Data Protection Reform, Art 15 in the proposed regulation on eID and trust services and Art 14 in the proposed Network and Information Security Directive.

Article 13a talks about risk assessments, security measures and incident reporting. The provider providing public communications networks or publicly available electronic communications services shall take appropriate security measures to minimize impact of security incidents on users and interconnected networks and to guarantee network integrity, thus ensuring continuous supply of services over the networks. Providers shall report significant incidents with impact on operation of services to their Regulator (NRA). NRAs can inform or require the provider to inform the public when

this is in the public interest. NRAs inform other NRAs abroad and ENISA when relevant, eg. in case of cross border incidents. NRAs provide an annual summary report to ENISA and the European Commission.

Art 13b gives the power to the NRAs to issue binding instructions, require providers to provide information needed to assess the security and/or integrity of their services and networks, including documented security policies, to submit to security audits and finally it empowers the NRAs to investigate cases of non-compliance on the security and integrity of the networks.

The electronic communications services in scope for reporting to the European Comimission and ENISA are fixed telephony, mobile telephony, fixed internet access and mobile internet access.

ENISAs role is to support an efficient implementation of the incident reporting - adhoc reporting to other NRAS and ENISA and annual reporting to ENISA and EC, to give feed back from received incident reports, which is done through an Annual Analysis of reported incidents and by giving recommendations on how to address significant incidents, and finally to support the NRAs in the sharing of experiences and in their task of requiring providers to take appropriate security measures.

ENISA is chairing an expert group of NRAs that meets three times a year and online with the common goal to work towards a hamonised approach of Art 13a. Together with the expert group ENISA develops guidelines and procedures and the experts in the group share information on past incidents, and discuss lessons learned and how to address certain incident patterns. Examples of outputs from the group are technical guidelines on security measures and on incident reporting.

Regarding reports to ENISA and the EC in 2011 and 2012 on incidents affecting the performance of ecomms services, most incidents affected mobile communications (mobile telephony and mobile internet). Only a small share of the reported incidents was due to malicious actions (6 % in 2011 and 8 % in 2012). The rest was unintentional causes like system failures, third party failures (power outages and cable cuts), natural disasters and human errors.

2.2 Auditing challenges for a national regulatory authority - Anacom Portugal

The telecom package has overall objectives to promote the internal market and guarantee citizen interests. Security in Art 13a belongs to this context.

Art 13a concerns the impact on networks, services and users. Measures have technical and organisational perspectives. They concern “significant” impact, without being defined. This has been done through the ENISA guidelines[1] and the NRAs interpret this further in their secondary legislations.

We engage in joint exercises, but they are mainly on malicious cyber incidents. We need to exercise in the most common threat scenarios, such as power supply shortages, cable breaks and natural disasters.

We need to cooperate across sectors, for instance with the energy sector. We need to understand the sector and to involve them in our work, we need to share information and we need contact points.

On audits, Art 13a is a regulatory model, not a certification model. Many standards available are on certification.

[1] The Article 13a WG technical guidelines on incident reporting, see References.

The sector is well prepared, so the audits should support security improvements and not take initiatives that cause problems. We also need to look at the sector's overall readiness. The notifications and audits are input to this.

The audits need to be both dynamic and long term because the environment is both fast changing and stable.

The knowledge of the auditors is crucial for meaningful outcomes.

Should the audits focus on continuous audits, on event driven audits, internal audits, self-assessments, what should be the targets, what critical issues or assets should we focus on?

Since there is no singular approach we need to work with audits in a triangular relationship between the NRA, the providers and the auditors.

We have five security regulations that have commonalities and differences. This needs to be discussed on a European level, otherwise there will be problems at national level.

2.3 Working with network security at Telecom Italia

When working with network security, the first thing to decide is to define what to protect, to classify the assets. Important is also to agree upon the ecomms assets with other providers.

The second step is to have a clear crisis management policy and procedure.

The ENISA Guideline on Security Measures are of good value here[2].

You have to work with incidents in a preventive manner. When it has started it's already too late to stop it, as it impacts with the speed of light.

There is a challenge with the shift from the old telecom model with intelligent networks and passive devices to unintelligent networks and intelligent devices. This affects the culture of the provider and the competence of the staff. We are now breaking out the network operation into one separate company, in order to separate the assets from the provider.

Another challenge is the increased use and trust in clouds, especially secure clouds for institutions.

There are some other challenges also, for instance, the role of the ISP during a malware attack either on a customer's device/system or on the provider itself and its services. For privacy reasons, we cannot tell a customer that his or her computer is infected. In other countries this is possible though.

For the joint work with overall security the private public partnerships concept is very important.

As we are interconnected in physical and logical networks, to protect ecomms assets there is a need for information exchange.

Ecomms providers should share information through NRAs, NRAs should share with each other, and the information should go back to the providers in an anonymised way. If you give information you should get information and vice versa.

2.4 Auditing security measures - KPMG Luxembourg

Security and privacy aspects are tied together. You should not separate them.

[2] The Article 13a WG technical guidelines on minimum security measures, see References.

Telecom is moving in different directions. It's not only about package switching, it's also about the development of services, of outsourcing, cloud services etc.

For auditors cloud services are treated in the same way as outsourcing.

When you outsource IT, you cannot outsource the responsibility. You are still responsible for your operations.

Security needs to work on an organisational, technical and process level.

A security policy gives guidance but it only makes sense if it's known and used. Security measures and controls are only meaningfull if effective in design (adequately built) but must as well be effective over the entire time (and not most of the time or when an audit is announced).

Regarding ISO, if the purpose is to state a minimum baseline accordning to predefined paramameters, then it's fine, but if you want to make sure that security is working, not only to show for the auditor, then maybe it is not enough.

SOC2, Service Organisation Control reports, was described, which is designed and established for the IT sector and critical areas. Big standards don't really address this.

The benefit with an auditor is that he/she is independent and is in some way liable to the audit result, as it affects the credibility of the auditor.

When performing audits, the audits need to assure that security measures are really working, and also for a continuous period, not only at the moment of the auditing.

There are different auditing frameworks. Certification is one part, but it is not enough, it's like a stamp. Then there are Agreed Upon Procedures, AUP – widely recognised auditing techniques. The challenge with AUP is that you define what to audit, which makes it difficult to compare between companies in a sector. Also it gives a snapshot, not a continuous picture. Then we have shared assessment programs, which is like a combination of AUP and Art 13a type security measures. This is still limited to a "stamp".

In Luxembourg a working group is taking shape with the ADPL (Association for Data Protection Luxembourg), NRA, DPA and the CERT. The ambition is to combine the elements in SOC2, which are defined as security, privacy, integrity and availability.

We are attempting to combine Art 13a and Art 4 into one context.

3 Highlights from the panel

The second half of the ENISA-ISACA workshop was led by a panel consisting of a representative from ENISA, ISACA and the presenters representing a national regulator, an electronic communications service provider and an auditor. The panel facilitated open discussion on a number of questions regarding the relationship between NRAs, providers and auditors, and between security measures, incident reporting and risk management.

Auditing isn't easy and carries with it a high degree of risk. Its more than just ensuring that control objectives are achieved. It requires expertise and building trust and confidence with business units. Once such trust is established within the company, audit can be quite useful.

It is very important that security risks are identified and that responsibility for their monitoring and mitigation is assumed at higher levels within an organization and that resources are prioritised.

Going forward security assessments are critical and are a mandatory requirement for improvement. Such assessments can be done internally as self-assessments, but third party and independent assessments are needed as well.

Auditing and the way NRAs work with auditing is part of a maturity process. It begins with a mandate to look for compliance with security. What follows are the establishment of high level security measures and requirements around incident reporting. Once information is collected it is reported and then can be used to identify and address specific types of incidents by sector. It's a learning process with auditing facilitating communication and being a part of the supervision process.

One of the primary benefits of an incident reporting framework, and/or a security measures guidelines framework is to reduce the cost of implementation in individual countries where you have multiple implementations of the EU Directive or business working cross borders. The next step is to further define and operationalize the role of auditing and supervision with the NRAs to ensure that supervision is performed in a consensus manner.

Guidance and frameworks don't need to be reinvented. Pick one that works for you (i.e. ITIL or COBIT), add on to it and take responsibility for it.

An important role that an auditor plays is that an auditor sees a lot of different companies and as such can make comparisons and intelligent recommendations. However, audit is just a part of it. In the end the regulator is the one who is responsible for enforcement.

The level of compliance, control and audit, to which organizations are subjected today are big, expensive and time consuming. However, at the same time, there has likely been a lack on the scope of the assessment in Europe with mobile telecommunications. More and more people are accessing the Internet through web applications and by means of mobile communications. We are now seeing similarity between the mobile networks and the ICT and SCADA networks. The level of risk on mobile networks is increasing, and there is a need to not only focus on DOS attacks, but properly invest in resources to address the third party side of the problem. With 4G there are more distributed elements of telecommunication networks which has increased the potential attack vector to central telecommunication networks.

It's not in the Directive, but security awareness and the knowledge must be increased. It's not only a question of sharing information, but also a question of how to process it. The NRA has a responsibility for creating and managing awareness of the overall picture.

Regarding auditing, one major thing to remember is that audit cannot be solely relied upon. Audit provides a baseline measure. There are different objectives to be addressed during an audit and usually audits are conducted at a pretty high level. This means that it's not going to go into the technical details of the system, operations of the system and how they are really developed and implemented. Audit is an excellent measure in support of security efforts.

There was a concern expressed around what might be discovered in performing an audit in the context of Article 13a. It was pointed out that one thing a regulator has to be well aware of is not to distort the market. We have to audit the operators, but in a different context. Operators need to be engaged with regulators to ensure consistency. You don't want one regulator saying one thing and another something else.

One of the challenges with security overall is that there aren't clear consequences for non compliance. Organisations are overwhelmed with regulations. The consequences for serious noncompliance have to be a serious part of that equation whether or not you have an audit as part of that process.

For bigger companies, as an output of their security governance process, there should be audits on specific security devices and audits conducted on the security governance process itself.

A business needs to be protected in depth and to be protected in depth there are three layers (management, security, external audit) and several steps to be performed, which may include an assessment on vulnerabilities, access control, alerting and auditing. Security is a matter that has to be taken into account by everybody in the company.

4 References

EU legislation

- The electronic communications framework directive incl Article 13a and b (incorporated in the telecom reform):

- In 2013 the European Commission issued a European Cyber Security Strategy and proposed a directive on Cyber Security. Article 14 of the proposed directive is similar to Article 13a, requiring operators to take appropriate security measures and to report significant incidents.

Related ENISA papers

- The Article 13a WG technical guidelines on incident reporting and on minimum security measures: https://resilience.enisa.europa.eu/article-13
- ENISA's report about the 2011 incidents, reported under Article 13a: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011
- ENISA's report about the 2012 incidents, reported under Article 13a: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012
- ENISA's whitepaper on cyber incident reporting in the EU shows Article 13a and how it compares to some other security articles mandating incident reporting and security measures: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu

Related ISACA papers

ISACA offers cybersecurity books, papers, studies and a Knowledge Center community. Visit *http://www.isaca.org/cyber* to access:

- **Advanced Persistent Threat Awareness Study Results**—More than 1,500 respondents worldwide share their APT concerns and describe their enterprises' ability (or inability) to handle an attack.

- **Advanced Persistent Threats: How to Manage the Risk to Your Business—**This book highlights key differences between the controls needed to counter the risk of an APT attack and those commonly used to mitigate everyday information security risk.
- **Responding to Targeted Cyberattacks—**This guide shares key tips for detecting and responding to an attack.
- **Transforming Cybersecurity Using COBIT 5—**This publication applies the COBIT 5 framework to transform cybersecurity in a systemic way.
- **Cybercrime Audit/Assurance Program—**The objective of this audit program is to provide management with an independent assessment relating to the effectiveness of cybercrime prevention and detection as well as incident management processes, policies, procedures and governance activities.
- **Cybersecurity community**—ISACA's Knowledge Center community offers discussions, wikis, documents and relevant links to equip cybersecurity professionals with the information they need.