EBU

OPERATING EUROVISION AND EURORADIO

R 144

CYBERSECURITY GOVERNANCE FOR MEDIA COMPANIES

RECOMMENDATION

SOURCE: SP-MCS

Geneva
September 2016

Page intentionally left blank. This document is paginated for two sided printing

Cybersecurity Governance for Media Companies

EBU Committee	*First Issued*	*Revised*	*Re-issued*
MCS	2016		

Keywords: Information Security, Cybersecurity, IT Security, Governance, ISMS

Recommendation

The EBU, considering that:

1. Media companies increasingly rely on information technologies and networks such as the internet.
2. The threat of cyberattacks is growing (and several broadcast companies have currently been successfully attacked);
3. Cyberattacks may lead to harmful damage for broadcast companies, and
4. Information security breaches in general may lead to impaired service delivery, reputational damage, non-compliance with laws and regulations, as well as to financial penalties.

Recommends that:

Media companies establish cybersecurity governance that includes:

1. Board and executive management commitment to cybersecurity policy[1].
2. Cybersecurity as part of business objectives and processes.
3. Definition of cybersecurity roles including financial resources. (See overleaf and **Annex A**).
4. Linkage of information security and corporate risk management activities, aiming at a cybersecurity maturity level of at least three. (See **Annex B** for definition).
5. An implementation of an **Information Security Management System (ISMS)** that follows the best practice set out in international standards such as ISO/IEC 27001, 27002 and in ENISA[2].

[1] The cybersecurity policy is usually contained in a brief document endorsed by executive management that contains:

- A Scope
- A statement of commitment by executive management
- A definition of Cybersecurity Roles
- Clearly defined CISO (Chief Information Security Officer) responsibilities
- CAI (confidentiality, availability, integrity) protection targets.

[2] European Union Agency for Network and Information Security.
https://www.enisa.europa.eu/publications/standardisation-for-smes.

Background to this Cybersecurity recommendation

The objective of information security is to protect information from unauthorized access, modification, disclosure, theft or destruction, irrespective of its form (e.g., electronic, printed or spoken). Cybersecurity, which focuses on information technology, is an important subset of information security. In this recommendation the terms cybersecurity and information security are used interchangeably.

Every (media) company that depends on IT and networks for its business should have a cybersecurity organisation operating within it to manage the company's cybersecurity policy. As a minimum this organisation must contain the following roles:

- CISO (Chief Information Security Officer).
- CSIRT (CyberSecurity Incident Response Team)
- SOC (Security Operational Centre)
- First and second level support that include security functions.

And optionally, the following roles:

- Regional or Business Unit IT Security Officers
- Information Security Board
- Internal Audit.

These roles and their responsibilities are explained fully in Annex A

Informative Annexes A and B are in attachment overleaf.

Annex A: Cybersecurity Roles and Responsibilities

1. Chief Information Security Officer (CISO)

The CISO has the overall responsibility for all information security related concerns of the broadcast company. He is equipped with decision competencies, with budget to perform audits, (depending on size and organization with a team) and is ultimately evaluating cybersecurity risks. The CISO is part of the middle management and is reporting to a member of the executive board or board of directors (e.g. the COO or CEO). Cybersecurity risks are also included into the corporate risk management process and therefore reported to the board of directors. Depending on the size of the organization the role of the CISO should be fulfilled with one full time equivalent that has enough know how and industry standard certifications.

The CISO also acts as liaison to government authorities that are responsible for cyber defence.

Cybersecurity is not limited to IT systems (office, management) but must encompass broadcast systems in general. Cybersecurity of these systems is the highest priority for the CISO of a broadcast company. In case the company's IT department is separated to the broadcast department, it is highly recommended that the CISO is not attached solely to the IT department.

2. Security Operation Centre (SOC)

The SOC represents the main operation for security equipment such as the firewall(s), IDS/IPS, proxy and SIEM (Security Information and Event Management). It is attached to the enterprise IT department and in its role as operation centre it implements and operates security required by the CISO and, if applicable, the regional IT Security Officers.

3. CyberSecurity Incident Response Team (CSIRT)

This role is usually fulfilled within a department that is responsible for cybersecurity incident detection and the organization of an adequate response to the cyberthreat. It also analyses the amount and level of vulnerabilities in information systems and technically monitors compliance with internal cybersecurity policies. It also ensures an overview on cybersecurity threats and vulnerabilities derived from the software and systems applied in the company.

Information analysed by the CSIRT is not limited to information and events from security devices (firewall, antivirus, IDS, etc.) but also from other elements of the IT infrastructure (especially the corporate directory service) and for organizations with higher cybersecurity maturity (see **Annex B**), business applications such as traffic and automation systems and support systems for financial management, HR management, etc.

It is recommended that the CSIRT does not directly operate security devices or technical equipment related to IT production (e.g. Firewall). This responsibility remains that of the SOC, which is nevertheless driven by the CSIRT for handling security incidents. It is recommended that the CSIRT functionally reports to the CISO.

The CSIRT must also be capable of securely detecting and reporting breaches of internal company regulations or national laws that could lead to disciplinary measures within the company up to legal investigations against the persons responsible.

It is recommended that a code of ethics be established to ensure a controlled operation of the CSIRT and that a reporting procedure for breaches is in place within the company. The CSIRT

requires very extensive resources and expertise in cybersecurity. These skills are generally scarcely available even in large media companies. It is therefore recommended that the internal CSIRT is complemented or extended by trusted external CSIRT companies that hold relevant international and national certification.

4. General first and second level support

For security implementation, the first and second level support is usually included in security processes to achieve harmonized and efficient results.

5. Regional/Business Unit IT Security Officer

The Regional/Business Unit IT Security Officer is an optional role that, depending on size or general organization of the company, may be needed. The role implements all corporate security policies in the responsible area (organization, subsidiary or region). This officer should functionally report to the CISO but may be staffed in the regional organization. Usually the Regional/Business IT Security Officer is fulfilled in part-time next to other roles and is responsible for the definition of specific cybersecurity policies within his perimeter.

6. Information Security Board

To run the security organization within the media company, a national committee or Information Security Board should be established consisting of all Regional/Business Unit IT Security Officers, the CISO and additional cybersecurity correspondents. The board itself should report to an adequate management board. The Information Security Board's objectives and competency and escalation regulations should officially be signed and approved by the board of directors.

7. Internal Audit

The role of the company's internal audit is usually located within a dedicated department that ensures the compliance of various activities to legal and standard requirements. The Internal Audit is usually not independent of the company but independence and objectivity are its main principles and therefore it should be attached organizationally or functionally to the board of directors. It is recommended that the internal audit also includes cybersecurity within its scope.

Annex B: Cybersecurity Maturity Levels

Cybersecurity Maturity Levels

The Cybersecurity Maturity Levels are based on the *Capability Maturity Model* that defines the general maturity in five levels ranging from Level 1 (chaotic) to Level 5 (optimizing).

Level 1 (Chaotic):

There is no documented responsibility for cybersecurity assigned; security in general is driven "ad-hoc", typically uncontrolled and reactive. If no CISO role is defined the Cybersecurity Maturity Level would typically be 1.

Level 2 (Repeatable):

The responsibility for cybersecurity is assigned and documented. Parts of the cybersecurity processes are managed in a reproducible manner as standard procedures. The overall cybersecurity management performance is still reactive.

Level 3 (Defined):

There is a formal cybersecurity policy in place that has been approved by the executive management and a documented acceptable use policy exists. Many processes are documented; they can be characterized as "standard" processes and are improved over time.

Cybersecurity processes should cover the following areas (best practice and international standards such as ISO/IEC 27001/27002, CSA Star, German BSI IT Grundschutz, NIST SP800-100 or Cobit should be taken into account):

- Asset Management
- Cybersecurity for Human Resources
- Infrastructure Security (including network, storage, operating system)
- Platform Security (middleware, databases)
- Software Security (including Secure Software Development)
- Audit Management
- Business Continuity Management
- Change and Configuration Management
- Cybersecurity Risk Management
- Identity and Access Management
- Security Incident Management
- Threat and Vulnerability Management

Level 4 (Managed):

There is a cybersecurity organization in place that is performing proactively. A formal cybersecurity risk assessment (e.g. following the ISO/IEC 27001 approach) is done regularly. Typically, some metrics are already in place to measure, control and optimize the cybersecurity processes. The maturity of the cybersecurity processes can be proved by regularly conducted self-assessments.

Level 5 (Optimizing):

The information security management system is validated by an external authority (e.g. official ISO/IEC 27001 certification). The main focus for all cybersecurity processes is optimization and improvement.

Questions for Guided Cybersecurity Self-assessment

Level 1:

- Do you have a CISO role appointed in your organization?

Level 2:

- Is the role of the CISO appointed and documented in your organization? Documentation should cover some key aspects of the responsibility of the CISO role.
- Are there already cybersecurity processes or requirements documented in your organization?
- Is their proactive analysis done to identify weaknesses to improve the overall cybersecurity?

Level 3:

- Is there a formally signed cybersecurity policy that has been approved by the organizations executive management? If yes, the policy should point out in minimum:
  - Scope
  - Commitment
  - Roles
  - CISO responsibilities
  - CAI protection targets (confidentiality, availability, integrity)

- Is a cybersecurity organization in place and functional? The cybersecurity organization should cover the following roles if applicable to the organization:
  - CISO (Chief Information Security Officer)
  - CSIRT (Computer Security Incident Response Team
  - SOC (Security Operational Centre)
  - First and second level support that includes security functions

optionally

  - Regional or Business unit IT Security Officers
  - Information Security Board
  - Internal Audit

- Are their cybersecurity processes documented and operational? Cybersecurity processes should cover the following areas (best practice and international standards such as ISO/IEC 27001/27002, CSA, German BSI, NIST or Cobit should be taken into account):
  - Asset Management
  - Cybersecurity for Human Resources
  - Infrastructure Security (including network, storage, operating system)
  - Platform Security (middleware, databases)
  - Software Security (including Secure Software Development)

- Audit Management
- Business Continuity Management
- Change and Configuration Management
- Information Security Risk Management
- Identity and Access Management
- Security Incident Management
- Threat and Vulnerability Management

Level 4:

- Does your cybersecurity organization behave proactive?
- Is there any regular cybersecurity risk assessment done (e.g. by following ISO/IEC 27001)?
- Are there any metrics in place to measure the effectiveness of cybersecurity policies and processes?
- Is there any regular self-assessment done to measure the maturity of the cybersecurity in your organization?

Level 5:

- Is your information security management system certified by an external authority?