eurofins | Cyber Security

CyberSecurity Framework: Media Edition

Safeguarding the Media Supply Chain: Technology, Processes *and* People

Eurofins Cyber Security's **CyberSecurity Framework: Media Edition** is a wide-ranging cyber security solution essential for all companies involved in

- Media Production
- Media Distribution
- Media Consumption

More and more media organisations are discovering increasing risks and vulnerabilities in the media supply chain. The Eurofins Cyber Security developed solution addresses business processes, technology and the need to give staff the ability to handle internal and external cyber security threats.

The CyberSecurity Framework: Media edition has been developed from the ground up to deliver cyber security across the supply chain. Our expert teams have identified the key security concerns for each of the sectors and developed solutions.

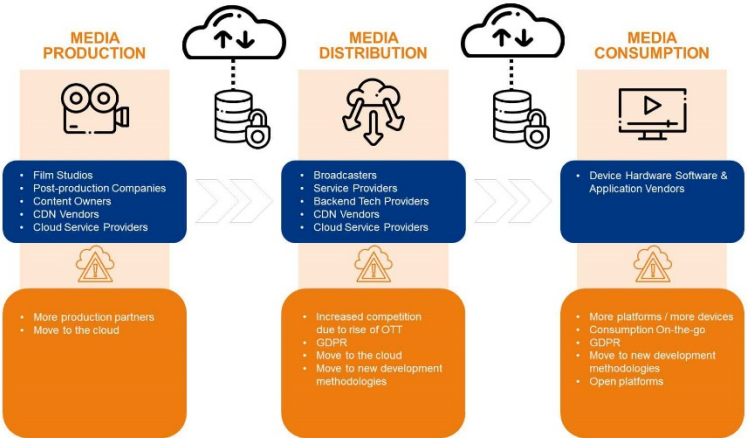
The Framework considers not only the processes and the technology but also the role of your staff. Too often the role of staff and colleagues is ignored in an audit but the Framework ensures that all members of staff are given the appropriate skills and are primed on identifying cybersecurity concerns at every turn.

Understanding the Challenge

The media supply chain for a production is extensive and many companies and organisations can be involved at different stages of an original concept being developed into a deliverable production.

The level of awareness of cyber security issues within those organisations can vary, from extensive down to limited. Those taking a lead in a project need to have the assurance that their organisation and all those that supply it are working in the most secure environment possible.

Illustrated below are the organisations that need to consider their cybersecurity robustness and the threats they face.



Inevitably, then, overall supply chain security can also vary significantly in its scope and its security. The ad-hoc testing undertaken by companies in the supply chain can deliver acceptable levels of security, but these may not be sufficient or optimised to the chain as a whole: they can leave potential vulnerabilities, exposing themselves or their suppliers/partners to risk. Any solution, then, would not have to address risks from processes and the underpinning technology but also that from people, often neglected audits.

The CyberSecurity Framework: Media Edition Solution

The CyberSecurity Framework: Media Edition was conceived as a solution to delivering the highest level of security across the supply chain:

'A consistent approach to end-to-end cyber security delivered by a single organisation in a single (but customisable) package.'

Addressing each stage of the Media Supply Chain

CyberSecurity Framework: Media Edition addresses the three consecutive areas in the supply chain:

- Media Production
- Media Distribution
- Media Consumption

Each has its own areas of vulnerability and each corresponding security solutions that we address. Following is an overview that illustrates the key security concerns for each stage, the solutions offered, and the additional functionality/ focus afforded by the CyberSecurity Framework.

	Key Security Concerns	Solutions	CyberSecurity Framework focus
Media Production	• Content is stolen or held hostage (Hack) • Content is unavailable or lost (Disruption) • Unauthorized copying of content (Piracy)	• Identity & Access Management (IAM) • Third party assurance of supplier security • End-to-end content protection & encryption (like DRM)	• Cloud security e-learning module • DPP readiness assessment • Supplier security audit (ISAE 3401) • Security assessment content storage (Pentest)
Media Distribution	• Content leaks or is stolen • Subscriber data is compromised (GDPR) • Service is unavailable of disrupted	• End-to-end content protection & encryption (like DRM) • Identity & Access Management (IAM) • Business continuity and disaster recovery plans	• GDPR e-learning module • DPP readiness assessment • Security audit (ISAE 3401) • DRM security assessment (Pentest)
Media Consumption	• Content leaks, copied or stolen (Hack) • Devices are compromised (Malware / Botnet) • User data is compromised (GDPR)	• Main focus on compliance: Digital Rights Management	• Secure development e-learning module • Security audit (ISAE 3401) • Device security assessment (Smart TV, STB, etc.)

The solutions offered by the CyberSecurity Framework: Media Edition deliver to companies involved in the supply chain, for the first time, a truly holistic solution, not forgetting the people in the organisation. In the Framework it is important that we consider staff, provide them (though e-learning programmes) with the skills and knowledge required for a cyber security aware business.

Benefits to companies in the Media Supply Chain

What benefits does using Eurofins Cyber Security and the CyberSecurity Framework: Media Edition bring your organisation, your partners and subsidiaries?

- Deal with a single partner, well respected in the business, for all your cyber security needs
- Consistent and coherent reporting of results across your supply chain
- Access to Eurofins Cyber Security assets for including e-learning programmes.
- Solutions extend end-to-end in the supply chain – or cover only the sections of the chain required by the business.
- Your potential partners, and subsidiary organisations, have the assurance that they are working with a company that puts cyber security to the fore and is always ahead of the game – and the cyber criminals.

About Eurofins Cyber Security

The Eurofins Cyber Security team has over 100 cyber security experts focusing on helping your organizations to ensure the continuity of their business, processes and devices by resisting cyber threats.

Eurofins Cyber Security is part of Eurofins Digital Testing, a global leader in end-to-end Quality Assurance (QA) and cyber security. We work with key high-technology businesses in the consumer electronics, software development, automotive, IoT, connected health and media markets.

We are also part of Eurofins Scientific, which has more than 800 laboratories in 47 countries and over 45,000 employees worldwide. Since its foundation in 1987, Eurofins has grown to be a highly-regarded organization with a level of expertise that makes its operations the first call for businesses around the world who are looking for the highest standards in testing.