Tailoring cybersecurity for the Broadcast Media industry

Trusted partner for your **Digital Journey**

Atos

“The shift right of the broadcast media industry”

Technology is changing everything, and the broadcast media industry is no different. The industry is on the cusp of a ‘perfect storm’ as a variety of factors – from customer demands through to evolving business models and services – combine to drive a radical transformation.
Firstly, the way content is consumed has changed dramatically: video on-demand and mobile services are now part of daily life. Traditional linear TV is likely to remain dominant for sometime, nevertheless audiences are fragmenting across numerous platforms – from social media to over-the-top (OTT) and streaming content providers such as Netflix, Amazon Prime and NowTV.

The traditional media value chain has been disrupted, enabled by the Internet and mobile connectivity, content is now expected to be delivered anytime, anywhere and on any platform.

To keep up with consumer demands and market threats, media organizations are scrambling to reshape their traditional business models and processes, consolidate operational procedures and make themselves as agile and customer-centric as possible.

From a technology standpoint, the industry is shifting away from bespoke broadcast hardware solutions towards software-based platforms, based on commodity IT and IP based infrastructures and networks that traditionally have been restricted to non-critical applications (e.g. monitoring and management). The move to a commodity infrastructure reduces support and capital costs, improving scalability & flexibility while allowing new technological breakthroughs not possible until now, i.e. by acting as an enabler for transition to 4k, 8k etc. IP can handle the bandwidth requirements more easily that traditional signals and cable types like SDI (Serial Digital Interface). This step is critical and has implications for the entire content supply chain, from production to final consumption. IP networks and IT systems are progressively playing a greater role within the core broadcast chain – for example in the IP routing and distribution of transport streams that would have been previously carried as ASI (Asynchronous Serial Interface) over coaxial cables; or in software applications that allow channel playout from virtualized IT infrastructure.

3 main challenges

Interestingly, **this switch of broadcast technology to IT and IP is both an effect and a driver** of the transformation mentioned above. TV service providers need to open their supply chain to the IP and mobile platforms **to expand their ability to reach their audiences** and they must have the capability to create new channels and enable new business models that will allow them to thrive in a severely disrupted market.

Broadcasters are under pressure to be **flexible and agile** in adopting new formats, creating new products, and supporting new delivery platforms. Finally, service providers will need to **reduce their operational costs** to regain a competitive edge, by streamlining and smoothing their processes : re-routing resources into more creative and consumer-centric investments.

This sounds simple but appearances can be deceiving. The standard IT processes and architectures must be properly adapted and deployed to meet the specific requirements of broadcast applications and operations in terms of service levels, reliability, business continuity and security.

1 The switch from SDI to IP is accelerating

Only recently standards have been defined to allow true operability and efficiency in the switch from SDI to IP as a feasible option. In this context, it's important to emphasize that the current need to transition from SDI to IP protocols is specifically relevant to live broadcasts and point of transmission. Pre-recorded content is already moved as files on IP networks - and the introduction of online services, like video-on-demand and live streaming, has already made IP networks a core part of the broadcast distribution infrastructure. Moreover, the digitization of workflows, enabled by the digitization of content from legacy physical supports (tapes, films, etc.) to digital files, has been going on for several years. Software platforms – running on virtualized IT environments – are already implementing media functions such as media asset management, file movement, quality checking and encoding.

2 Broadcasting and IT: two converging worlds

In these evolving technical and operational scenarios, more and more broadcast engineering departments are facing the challenge of building, managing and securing their own IT – from data centers through to networks – sometime in cooperation with the IT departments, sometimes independently. This determines the need to inject new resources into the organizations that should be able to combine the skills and competencies of the two converging worlds: broadcast and IT.

As the role of IT and IP is growing in the broadcast media segment, cybersecurity risks are impacting content, customer data, service and business continuity. Legacy broadcast technology infrastructure used to be isolated and mainly hardware based, so less exposed to cybersecurity risks. But now broadcast functions are increasingly based on software and connected to internal and external IP networks and thus are potentially insecure if proper preventive and reactive actions are not taken to mitigate and to manage those risks.

Consequently, media companies also need to develop a whole new area of competence in cybersecurity, a topic no longer relegated to IT departments, but that is now a business priority.

It's not just about protecting content assets, or at least guarding against unauthorized usage. It's not even about ensuring that the confidentiality on millions of registered customers is respected. It's also about securing the wider infrastructure itself. When hackers can now power down an electricity network by targeting the operation and machine control network, they can do the same to a media enterprise.

The good news is that the media companies don't have to reinvent the wheel: they can leverage the tools and best practices that other industries already being applied for many years in mission critical scenarios.

> "It's not that we are re-inventing the wheel on cybersecurity," "We just customize it for media organizations."
>
> **Adi Kouadio**
> The EBU's Lead on Video R&D and Cybersecurity.

The industry is looking for standards, reference architectures and best practices to reduce the risk and to properly direct the future investments around technology.

3 Broadcast Media security concerns

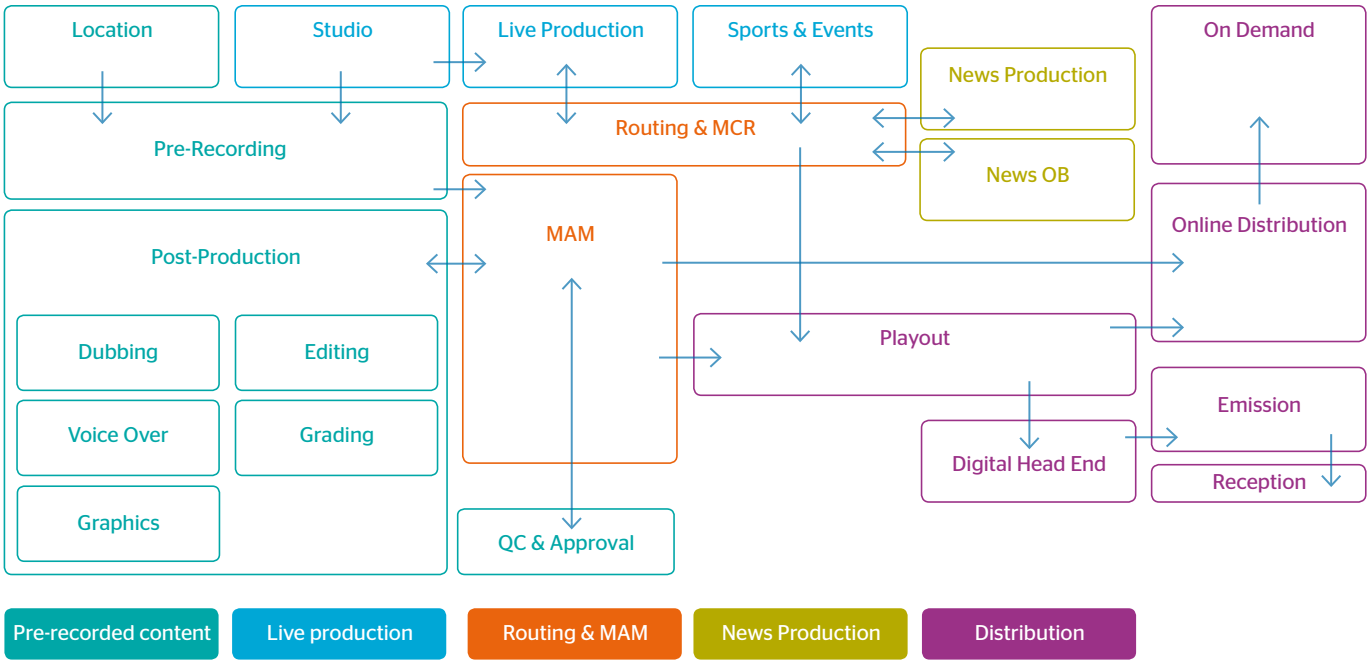
We can classify the main security concerns of the media companies into two categories:

Enterprise IT (data centers, network applications, etc.) security concerns, which are common in all the industries.

Broadcast media security concerns, which are specifically related to the core business activity of the broadcast media companies. Given that cybersecurity in the context of Enterprise IT is applicable in essentially the same way across all the industries, including the broadcast media segment, the focus of this paper is around the second category. There are some peculiarities of the cybersecurity in the broadcast media, in terms of the security risks and the related tools, as well as best practices and services to avoid or mitigate those risks across the whole broadcast media supply chain.

The Broadcast Chains

A typical broadcaster has to manage a mix of live and pre-recorded content on different technology stacks for distribution on multiple platforms creating a variety of interlinking broadcast chains.



Live content is delivered from a variety of sources including studio, location, news story, sports venue or event with live feeds distributed as real time video signals on a wide range of links. An internal studio may link by facility SDI tie line or external studios and Outside Broadcasting (OBs) can connect by private link, telco provided link or satellite or radio link. These increasingly utilise IP as a transport even if presentation is in a traditional format. In the future we expect to see more IP to IP hand-off.

Pre-recorded content may be created in a studio or on location and typically follows a workflow with media stored as IP files and distributed to multiple post-production systems and providers. Files are managed by on premise or cloud based Media Asset Management (MAM) systems that may also control other non-linear systems such as libraries and archives. Post-production of recorded content is now well established as a digital file-based process with multiple digital processes available from many providers including cloud-based services. Specialist dedicated news systems replicate standard functionality provided for live and pre-recorded content with all of the technological diversity but tailored to the specialist needs of news production.

Distribution functions combine live and pre-recorded content for channel play-out. Coding and Multiplex systems prepare linear channels for traditional emission as well as online distribution. Pre-recorded content and post broadcast live content may be made available to on-demand platforms. Traditional distribution technologies are increasingly adopting IP platforms with some linear channels already moving functions into the cloud alongside the on-demand processes.

Chain concerns

A broadcaster's security concerns change as content moves through different parts of the production chain. **Confidentiality** is typically more important early on in the production chain for example where a broadcaster may wish to protect the plot development of a major drama or the source identity for a news story. Confidentiality is rarely a concern for live programmes or events, however it is important to **manage access** to broadcast content for paid services which would fall under the confidentiality banner from a security perspective. Free-to-air broadcasters have few confidentiality concerns for distribution.

Integrity and Availability are important factors for broadcasters in production as with other business systems. The wrong content or unavailability of content could have business implications and incur production costs as work is delayed or has to be repeated. In distribution Integrity and availability often become critical for broadcasters. Loss of transmission removes a broadcaster's revenue stream or is reason for being the wrong content or hijacking the airwaves can gave an even greater impact. In either case the broadcaster may suffer reputational damage, incur political or regulatory sanction and incur financial loss.

Key Risks & Weaknesses

Control and management of broadcast systems and content is reliant upon IP networks often connected to the internet for support. Content is also transported or stored on public networks or systems.

Control the access

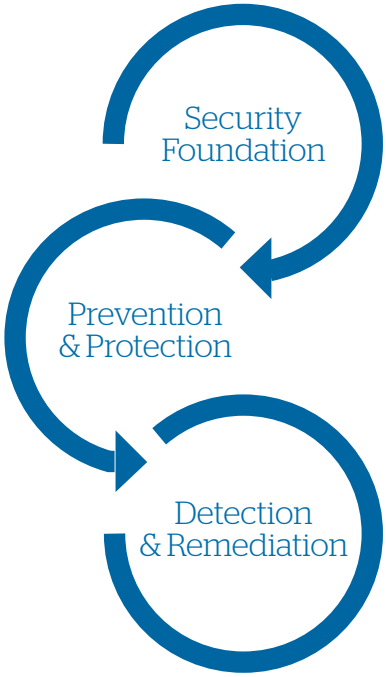
The nature of the modern broadcast chain provides many people with access to information and to systems. Audiences and visitors may be on-set or location for a recording and may have their own personal recording equipment in the shape of a mobile phone. Staff working on a production may be employees of the broadcaster, contractors, freelancers or work for a 3rd party service provider. They will require different levels of access to the content or broadcast systems.

Broadcaster regularly need to share content with each other which for pre-recorded IP content necessitates file sharing and for live IP traffic requires connecting networks together.

Sharing content

The content itself and associated collateral may be shared between companies for processing and distribution. For live media this may be through a telecom provider and for recorded media any number of post-production service providers may require access to the content or the ability to download the content for processing. Some content may be transported over the internet as live streams or files. Broadcasters regularly need to share content with each other which for pre-recorded IP content necessitates file sharing and for live IP traffic requires connecting networks together. With IP based content this requires connecting multiple networks for live streams or sharing files for pre-recorded content.

How to Secure the Broadcast Media Sector: Where to start?



Security baseline definition and risk assessment
First and foremost is to set up a solid security foundation covering the Broadcast Media production chain end-to-end, including people, processes and technology.

No need to reinvent the wheel, just follow best practices coming from the IT world: NIST Cybersecurity Framework, COBIT (Control Objective over Information and related Technology) or ISO 27K series. Any of those will do the work, just pick & choose the one which aligns better with your corporate policies. There are also dedicated Broadcast Media cybersecurity standards arising which would be good to explore:

- DPP Committed to Security Programme
- CDSA Content Protection & Security Standard
- MPAA Content Security Best Practices
- EBU places a significant effort to publish recommendations on very specific cybersecurity concerns in Media: Vulnerability Management (R160), Cloud Security for Media (R146), Mitigation of Ransomware and Malware Attacks (R145),...

Digital Production Partnership (DPP) holds a specific programme named "Committed to Security" which promotes best practice in cybersecurity across the media supply chain. It is based on two major initiatives: a Supplier Security Checklist, generated by DPP members, and the Broadcaster Cybersecurity Requirements created in conjunction with NABA (North American Broadcasters Association).

Once a security baseline is in place then you need to strengthen the security controls based on proper risk assessments of your Broadcast Media assets. Address each of them consistently but also prioritize your specific areas of concern.

After analyzing the cybersecurity concerns in the different parts of the production chain and the motivations of the different cybercrime groups, we have come up with the following list of major focus areas to secure the Broadcast Media industry:

Protect content:

- valuable data whether latest movie or TV series: This content IS the business - it generates the cash flow and has critical shareholder value
- journalistic informant investigations (protecting your sources is critical for your credibility on the market & for the safety of your informant)

1 Protect the Brand:

Industry secret leakage, internal communication leakage will impact brand or fake-news distributed without proper review/ authorization.

2 Protect consumers' private identity information:

Content is delivered online and through different means like data analytics and AI, which could provide access to very critical private information of their consumers.

3 Protect employee data:

This should be a top priority, including the reporter's geographical location when in the field.

4 Protect the broadcast infrastructure:

Avoid failures, misconfigurations, human mistakes and, of course, cybersecurity attacks that could have a negative impact on service continuity and quality.

5 Fraud detection

Illegal access to online content. Even including Curbing Pirated TV/Satellite piracy (although this is not a cybersecurity issue).

6 Laws & regulations compliance and standards adherence

With the risk assessment complete and your focus areas allocated, then build a comprehensive Cybersecurity strategy that covers both prevention & protection and detection & remediation.

[1] https://www.thedpp.com/tech/security/committed-to-security/
[2] http://www.mesalliance.org/wp-content/uploads/2016/04/Content-Protection-Security-Standard-February-2016.pdf
[3] https://www.mpaa.org/wp-content/uploads/2015/11/MPAA-Best-Practices-Common-Guidelines_V3_0_2015_04_02_FINAL-r7.pdf
[4] https://tech.ebu.ch/publications


23:59:59:24

Prevention & Protection

Prevention & Protection strategies must be implemented once there is a strong enough security foundation in place. Prevention security controls will avert the threat before it occurs. Protection security control takes over when prevention fails. Protection controls are a combination of security equipment and safety procedures that are used to defend against and eliminate threats. Prevention and Protection are different, but both must be used simultaneously to secure your Broadcast Media business from possible threats.

Below there are some Prevention & Protection security controls examples. Nevertheless, those need to be reviewed -and extended- to match your specific security requirements:

- **Build a cybersecurity culture:** educate, educate, educate... Your own personnel first, but also your providers and your customers when applicable.
- **Develop your end-to-end cybersecurity strategy and keep it up-to-date:** know what your critical assets are, your crown jewels, devise a strategy to protect them, implement such security controls and monitor continuously for its effectiveness.
- **Secure the extended Enterprise:** Secure the entire supply chain (multiple partners are involved in media industry from subcontractors, to partners, etc...) look at the Extended Enterprise. **The perimeter has vanished; you are only secure as your least-secure supplier.** Some security controls that might help:
  - **Data Loss Prevention Solutions to protection from IP rights infringement:** To watermark critical content and control access to content and identify the culprit if data is inappropriately used or even leaked. Piracy deterrent solution.
  - **Encryption of Data:** encrypt sensitive content, encrypt sensitive communication. If the network is compromised, data would be encrypted and not possible to access.
  - **Protection from Denial of Services attacks:** Anti DDoS Solutions to make sure online content and websites are always available and resistant to any type of DDoS attack.
  - **Identity & Access Management** solutions to define and manage access rights and to secure auditability of who have access to what and why.
  - **Security Processes** for patch management, password management, access control etc.
- **Integrate security concerns early in each innovation** considered as part of the digital transformation journey of the company (mobile apps, social media, OTT, infrastructure virtualization, wearable technologies). Security should be part of the initial design. Some security controls to consider from scratch:
  - **DRM solutions** to push digital right management on online content.
  - **Encryption of data** and even encryption of machine-2-machine communication (e.g. Internet of Things technologies are expected to grow quickly both on the Broadcast Media production and the consumer sides).
  - **E-transaction security,** especially whenever online payments are involved.
  - **Privacy for consumer data** used in big data solutions/projects.

Vulnerability management and penetration testing to make sure data is secure through all the development life cycle -including delivery.

Detection & Remediation

As effective as prevention and protection may be, it is not enough. As cyberthreats rapidly proliferate and become more complex, having a static set of security controls in our Broadcast Media chain will not be sufficient. While prevention and protection layers are still essential in stopping most commoditized threats, the Broadcast Media industry cannot rely on those layers alone - a determined attacker will find a way to breach even the most secure system. Prevention technologies alone can't stop highly targeted, sophisticated and multi-staged attacks. Targeted attacks such as spear phishing or social engineering are almost impossible to prevent: with employee and social media accounts, and all the Media business' third parties in the chain, there are too many attack vectors to exploit.

Therefore Detection & Remediation controls are mandatory. Some hints to consider:

- **Digital Surveillance** (targeted threat intelligence): to check on the dark web and beyond any piracy related activities. Or cyberattack preparations against the industry or breach discussion concerning the targeted company. Or online campaigns that could impact branch/ reputation. A 24/7 watch team should be created.
- **Proactive detection:** Vulnerability assessments, penetration testing, security audits, to detect vulnerabilities before they are exploited by hackers.
- **24/7 monitoring** of critical assets to identify in real-time any potential attempts to access your systems and crown jewels, aka intellectual properties and beyond.
- **Forensics to reverse engineer** cyberattacks and provide the digital proofs sustainable in a court of law for the prosecution of cyber-attackers and pirates.
- **Cyber Insurance:** to cover cost of cyber incident management, loss of data, business interruption, legal reliability etc.
- Finally, please consider **Recovery** as part of your Remediation strategy: a perfect cybersecurity system does not exist. A cybersecurity strategy should be formulated with the idea that breaches are inevitable sometime and anywhere within your Broadcast Media production chain. Broadcast Media organizations need to recognize that at some point their systems will be compromised so they need to get ready for that with the suitable controls and recovery plans.

How Atos can help?

Atos, a Trusted Partner

5000+ security professionals

125 million security events managed each hour

14 Security Operations Centers

1.37 million unique IPs scanned for vulnerabilities

3.2 million endpoints secured by Atos

3.5 million IoT devices secured

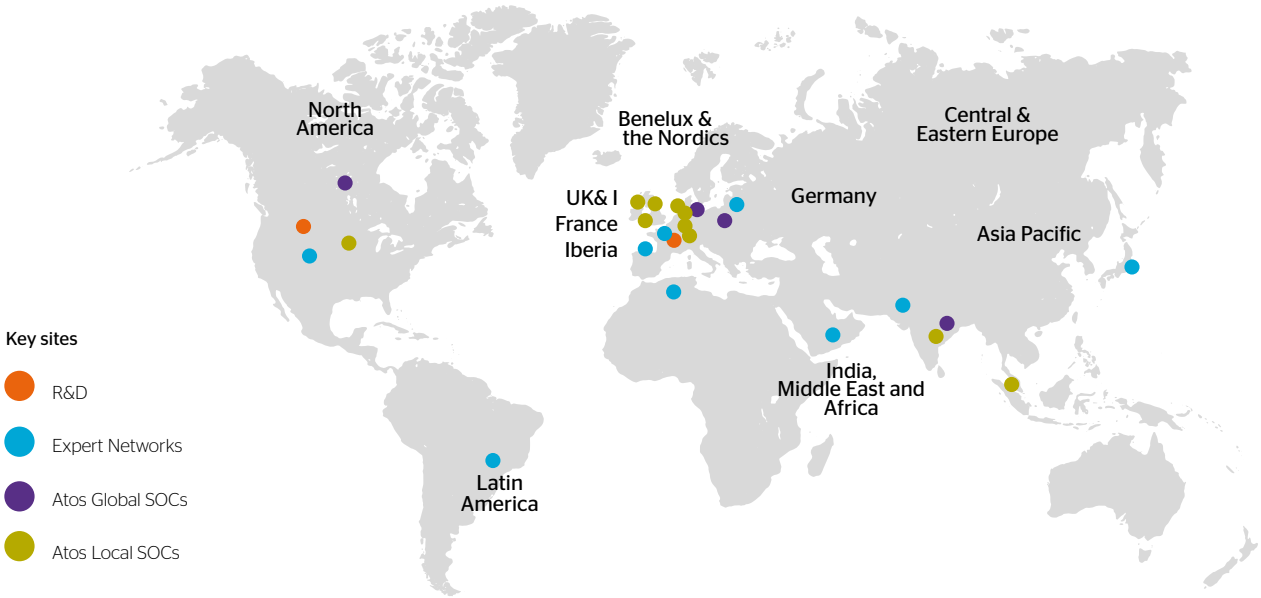
Evidian Identity and Access Management

Trustway Data Protection at rest and in motion

Horus Trusted identities for people and devices

LEADER	LEADER	NICHE PLAYER	3rd	NICHE PLAYER	LEADER	LEADER
IDC	NelsonHall	Gartner	Gartner	Gartner	teknowlogy	kuppingercole
Managed Security Services Europe	Managed Security Services WW & EMEA GDPR Services WW	Identity Governance & Admin WW	Managed Security Services WW Market share	Access Management WW	Identity Provisioning Global	IT Security Europe

- Atos offers "best of breed" cross spectrum security services as our services are based on the leading security solutions, independent of the hardware layer, and our own specialized cybersecurity product suites (Encryption with Trustway, Identity & Access management with Evidian software suite, IOT security with Horus, secure smartphone etc...).
- Atos is a leading European Managed Security Services Provider, recognized by leading analysts. Gartner praised Atos for its experience in integrating security services with complex, large-scale IT programs as detailed in Gartner's Market scope for European Managed Security Services Provider, for four years in a row.
- Atos has 14 SOC worldwide operating 24/7 with CSIRT (Security Incident Response Teams) ready to intervene to block and neutralize any attack in real-time limiting the attack impact.
- Atos has a core set of Global customers and demonstrated know-how in managing security environment for its customers.
- Atos has end-to-end capabilities to address all customers' needs from managed security services, to Consulting to Project Integration which is cost-effective for the customers.
- Atos security experts have developed extensive expertise in the security field and are committed to sharing their expertise with the customers.
- Atos understands Media & Broadcast. Atos Syntel's Media Practice is staffed with experts who have extensive experience not only in Enterprise IT but also in the Media and Broadcast processes, operations and technologies and the related latest industry standards and best practices.
- Atos is committed to innovation and has been leading security innovation programs for the European Union for the past decade.



About Atos

Atos is a global leader in digital transformation with over 110,000 employees in 73 countries and annual revenue of over € 11 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology space. Its expertise and services support the development of knowledge, education as well as multicultural and pluralistic approaches to research that contribute to scientific and technological excellence. Across the world, the group enables its customers, employees and collaborators, and members of societies at large to live, work and develop sustainably and confidently in the information technology space.

Find out more about us
atos.net/en/solutions/cyber-security
atos.net/en/industries/media

Let's start a discussion together

For more information: **mauro.starinieri@atos.net**

CT_J2844_190820_RY_B_TAILORING