Considerations in the Transition to IP Production Facilities

Version 7

Strategic Objective

A broadcaster's transition to new IP production facilities should be managed as both an executive priority and a strategic objective of the organization.

Technical References

Staff driving the move to IP production facilities must be knowledgeable in the following areas:

- SMPTE Media Transport over Managed IP Networks (https://www.smpte.org/standards/st2110)
- Cloud Technologies, Such as SaaS, PaaS, etc.
- Precision Time Protocol (PTP)
- Cybersecurity Frameworks, such as NIST, etc. (https://www.nist.gov/cyberframework)
- EBU Technology Pyramid for Media Nodes (https://tech.ebu.ch/pyramid)
- JT-NM Reference Architecture, TR-1001-01 and Test Plans (https://www.jt-nm.org/reference-architecture)

Considerations

Information Security

- Information Security should be a key component of the design, implementation, and eventual operation of the IP production project.

- Broadcasters should update vendor default credentials for all involved systems.

- Passwords and access keys for service and administrator accounts should be rotated in accordance with the broadcaster's Information Security policies.

- Elevated administrator privileges should be removed. Users should be provided role-based access only.

- As the move to IP will enlarge the cyber attack surface for threat actors, Information Security training should focus on implementing enterprise-wide behavioural change on the part of the employee and should be performed on an on-going, proactive basis. Further, employees should be trained to adopt a "zero-trust" attitude toward external requests.

- The reliance on cloud services becomes even more prevalent and important with the move to an all-IP infrastructure. Broadcasters need cloud security as they implement their digital transformation strategy and incorporate cloud-based tools and services as part of their IP infrastructure. In addition, the use of diverse cloud service providers is recommended.

- Traditional high-availability systems may not provide protection for certain cyber attacks as malware can be replicated in backup systems. Traditional backup/recovery programs need to be matured, to ensure "clean restorations" are achieved and recoveries can be accomplished. In addition, any back-ups should be sufficiently firewalled, or even "air-gapped" from main systems.

Architecture

- Effectively communicating the new IP architecture and design to all effected employees is crucial to gaining their alignment.

- Network segmentation should be a key component of the design, implementation, and eventual operation of the IP production facility in order to protect critical broadcast systems.

- Solutions should be engineered to run on currently-supported versions of Operating Systems. Solutions running on unsupported OS are unable to be patched for latest security vulnerabilities.

- Cybersecurity needs to be in lock-step with the architecture of the IP production system rather than being an afterthought.

- Zero-trust is the emerging cybersecurity strategy, but broadcast/engineering technologies do not tend to co-exist easily with even the most traditional cyber controls, so a viable adoption strategy is important when considering this approach.

- Privileged Access Management (PAM) technologies should be considered to control access to critical accounts, systems, and data.

- Change management/control should be implemented for scheduling/tracking/verifying/auditing all changes to critical broadcast and non-broadcast systems.

- A comprehensive, widely-disseminated IP architecture and design is very important. Without this, some internal teams may continue to work as they've always done. Changes made to existing non-IP infrastructures might be done temporarily with the intent to return with a final solution, but this might never occur.

Business Continuity Planning

- Broadcasters should rely on their Business Continuity Plan (BCP) and associated strategies to prioritize how to recover in the event of a cybersecurity breach. As such, cybersecurity plans should form part of the organization's overall BCP.

- Cyber incident response should trigger the BCP process early in the discovery process to ensure planning, business impacts and recoveries can be proactively addressed and coordinated with the cybersecurity team.

- Broadcasters' BCP's should be predicated on highly-available systems being available throughout the production chain, including origination facilities.

- Vendor BCP & Disaster Recovery Programs (DRP) must be reviewed by broadcasters at a deeper level to ensure they also are maturing traditional DR strategies to accommodate cybersecurity.

- When vendors manage critical business processes for broadcasters, a strategy to ensure broadcasters' access and availability to data and critical business information is an essential part of vendors' BCP strategy.

Vendor Risk Management

- Vendor risk management is a critical consideration for the enterprise given how broadcasters rely more and more on third parties as part of the IP supply chain.

- Vendors must adopt the latest security standards (e.g., MFA, antivirus, etc.) and integrations with third-party platforms (e.g., logging, monitoring, etc.)
    - Define roles and responsibilities for maintaining vendor solutions
    - Document password rotation procedures
    - Document vendor responsibilities versus customer responsibilities (e.g., patching, etc.)

- Broadcaster's comprehensive vendor risk assessment program is essential.

- Wherever possible, physical technologies should be inspected for tampering and should only be sourced from trusted/reputable vendors.

- Vendor cloud technologies should be assessed by the broadcaster to understand controls, certifications and integrations with other third parties (e.g., AWS, Azure, GCP platforms, etc.)

- Vendor access should be scrutinized, reviewed regularly, and provided based on the principle of Least Permission (PoLP).

External Consultants

- Experienced external consultants can be very helpful in developing the strategy and architectural design of the IP production project.

- External consultants should have adequate staffing to support broadcasters during implementations and operational cutover.

- If improperly managed, the risk in employing consultants or professional services is that there may not be the opportunity for full knowledge transfer. When these consultants leave, the knowledge might leave with them.

Training

- Repeated, progressive training in the new IP technology is essential to the success of the project.

- Radio and Television production teams' workflows will be dramatically changed with the move to new IP production facilities. They will need to be supported from the start of the project to ensure they continue to be "on-board" with the new facilities and processes.

- Considerations must be made for those who maintain 'legacy' production systems as many fundamental IT principles may not be common knowledge for them. The training curve for these individuals may be high.

- General cybersecurity awareness training should be mandatory for all employees with focused exercises for users with privileged access.

- Maintenance and operations staff in IT/Engineering teams will be the most affected by the move to IP production facilities. They will need to be trained on the "best practices" in operating and maintaining the new IP infrastructure.

Supply Chain Security

- Broadcasters must fully analyze and quantify the performance of every new device or service connecting to the new IP production project. Given the supply chain security breaches that have occurred in the past few years, vendors must now be thoroughly investigated.

- Broadcasters must address vendor requests for SaaS connectivity, which is no longer just an encompassed solution sitting only inside the network. Vendor solutions must now communicate with a cloud or a SaaS service in order to maintain licensing, advance logging analytics, etc. with AI and machine learning based off of what is happening inside the environment.

Networking

- Network segmentation should be a key component in the design, implementation and operation of the IP production project in order to protect critical broadcast systems.

- New IP infrastructures are typically characterized by the ability of any network device being able to communicate with another and potentially with outside systems, like the cloud. Enterprise staff must be well-versed in IP network engineering, design, protocols, technologies, etc.

- New IP network architectures should align with zero-trust principles (micro-segmentation) wherever possible. When micro-segmentation is not possible, the general segmentation of like systems to smaller networks should be considered.

- Bastion hosts and firewalls should be deployed between production and non-production networks as a best practice.

New Organizational Structures

- Ideally, structural reorganization should be done prior to the move to IP to ensure teams are aligned after the transition. Some organizations may opt for a different approach by deferring wholesale organizational changes as they perceive these to be too disruptive to employees, the corporate culture and their bottom line.

Version 7
June 26, 2023