# Cyber Security Hygiene in IP Broadcast Systems

Denis Onuoha – Chief Information Security Officer
Arqiva LTD

# Introduction

**Arqiva is a leading UK communications infrastructure company enabling a vibrant digital economy. We are behind the scenes and central to millions of vital connections. We are pioneers in an always on, always connected world.**

Every day our infrastructure and associated services enable millions of people and machines to connect wherever they are through TV, radio, mobile and the Internet of Things (IoT).

Our technology enables us to work with everyone from mobile network operators, such as BT-EE, Vodafone, O2 and Three to independent radio groups and major broadcasters, such as the BBC, ITV, Sky, Turner and CANAL+ to utility companies such as Thames Water.

Denis Onuoha is the Chief Information Security Officer at Arqiva. He has the overall responsibility for Security Risk Management, Information Assurance and Cyber Security for the company and is at the forefront of its fight in defending against the latest media industry cyber-attacks. Denis commenced work in the financial sector with responsibilities for Risk and Information Security, subsequently making the move across to the broadcast industry. He is a qualified Lead Auditor for the ISO27001 and ISO22301 standards; a Lead Implementer for ISO22301; a Risk Manager in accordance with ISO27005; and has successfully attained ISACA’s CISA and CISM certifications. A proactive IT professional, Denis sits on three of UK's Centre for the Protection of National Infrastructure (CPNI) Government Information Security Exchanges and is the elected Chair of the AIB Cyber Security Working Group.

# Moving to IP Broadcast Systems

- The merging of the broadcast, telco and computer industries has brought a lot of new technologies into broadcast systems.

- Video production, playout and transport is increasingly moving to IP-centric solutions.

- Once a provider identifies IP architecture is viable, they should outline the consumer experience, **security** and flexibility benchmarks they want to meet before embarking on the transition to a more IP-centric platform.

- This is an evolution and progression of technology from analogue to digital extending currently understood methods of IP network access.

- Moving to IP may require shifting to a new end-to-end infrastructure.

- IP based delivery has tremendous upside when configured and implemented correctly.

# Why is Cyber Security important for IP Broadcast Systems

- To protect company assets.
- To gain a competitive advantage.
- To comply with regulatory requirements and responsivities.
- Staying in business .

# Build / Operate and Maintain security for IP Broadcast Systems

Many customers take it upon themselves to mend security issues at their own sites.
Due to inherent limitations within legacy non IP systems, fixing security issues typically needs restrictive procedural controls: restricted access from remote terminals; restricted physical access to native terminals; additional login accounts; frequent password changes; automatic disconnect when periods of inactivity; and centralised logging call-back devices.

- Vendors of IP Systems now include purposeful security measures into their Broadcasting devices as standard Security which are not included in legacy equipment.

**Security Functions:** *What protection options will it provide?*
**Security Assurance:** *How  fool proof are the protection features?*

Extensive processes and procedures with operational instructions are documented for the security service.

Security operations should be evaluated often to identify potential gaps and critical areas for improvement.

# Basic security hygiene for IP Broadcast Systems

- Have a approved Security Policy that is enforced
- Physical security controls must be in place (i.e. Device Placement)
- Designing the IP network the proper way from the start is important to ensure that the network is stable, reliable, and scalable
- Be sure that strong authentication and password policies are in place to secure access to the device / operating system and configuration files; users have the minimum level of access
- Change the default passwords on the devices
- Do not deploy devices / managed switches using their default configuration
- Scan equipment using Vulnerabilities Assessment tools before and after deployment;
  - Harden device
  - Close insecure and unused protocols, services and ports
- Audit / Logging / Non-Repudiation

# Further security considerations for IP Broadcast Systems

- Is there communication gap between security and other teams.

- Broadcast security does not only concern devices at each end of the communication chain. The communication channel should also be secure.

- With IP networks and the Internet exposure network-based security attacks increase. (This exposure already exists with legacy kit connected to the enterprise network)

- There is a need to ensure that your IP network and services remain available and that the *confidentiality* and *integrity* and *availability* of the information transmitted remains intact.

- Perform a Risk Assessment.

- Gather an understanding of the many threats and vulnerabilities.

- Determine which parts of the back-end and network to upgrade to IP.

- Defence-in-Depth and Penetration testing is included within the project plan.

# Main technologies used to reduce the attack surface

**Firewalls:** A firewall is the first line of defence for the network.
**Switches / Routers:** Segment different networks traffic (management from data)
**Load Balancers:** distributes the IP workload among multiple servers
**Proxies:** a go-between for the network and the Internet.
**Web Security Gateways:** a single point of policy control and management for web-based content
**VPN Concentrators:** provides a secure method for remote access to resources
**NIDS:** Analyse data, identify attacks, and respond to the intrusion.
**NIPS:** prevents attacks instead of only detecting the occurrence of an attack.
**Protocol Analysers:** gathering packet-level information
**Spam Filter:** checking email messages when they arrive quarantines mail based on value.
**Unified Threat Management Appliances:** contain spam-filtering functions and can also provide antivirus protection.
**URL Filter:** Internet activity content filters
**Content Inspection:** monitors every packet of traffic that passes over a network.
**Malware Inspection:** a web filter applied to traffic that uses HTTP.
**Web Application Firewall:** protect web server from common attacks.
**Application-Aware Devices:** examine application traffic and identify threats through DPI.

# Conclusion

Good Cyber Security Hygiene results in:

- Reduces undocumented & unplanned changes meaning reduced avoidable outages and in turn less service credits
- Ensures consistency across all departments
- Solidifies into a single disaster recovery plan with the potential of cloud based recovery during a destructive denial of service attack
- Makes Good Business Sense as the customers will know you have done your best to secure their interests

?

Any questions

**Denis Onuoha**

Email: [Denis.Onuoha@arqiva.com](mailto:Denis.Onuoha@arqiva.com)

LinkedIn: [www.linkedin.com/in/denisonuoha](http://www.linkedin.com/in/denisonuoha)

Mobile: +447814219954