Cybersecurity Status Report

ABU Technical Committee Meeting

November 24-25, 2020

NABA

NORTH
AMERICAN
BROADCASTERS
ASSOCIATION

Contents

- NABA Cybersecurity Recommendations
- EBU Cybersecurity Recommendations
- World Broadcasting Unions
- WBU Technical Committee Cybersecurity Recommendations
- Cyber Threats to the Media/Broadcasting Industry
- Broadcasters, Media Vendors and Cybersecurity

Cybersecurity

“Cybersecurity Ventures, a trusted resource for cybersecurity statistics and predictions, predicts global cyber crime costs will reach $ 10.5 trillion by 2025.

“This would more than triple the $ 3 trillion in cyber crime in 2015 and represent a 15% annual increase for each of the next five years.

“To put it in perspective, this would greatly exceed the annual damage from worldwide natural disasters. This would also be more profitable than illegal drug trade worldwide.”

ISACA Smartbrief on Cybersecurity, November, 2020

NABA Cybersecurity Recommendations - Published

- Cybersecurity Recommendations for Public Cloud
- Cybersecurity Recommendations for SaaS (Software as a Service)
- Best Practices in an Effective Enterprise Anti-Phishing Program
- Best Practices to Mitigate Social Engineering

Available for free at: https://nabanet.com/cybersecuritysubcommittee/

NABA Cybersecurity Recommendations - 2020

- Cyber Protection of Personnel Operating in the Field (P2)
- Disaster Recovery Planning (P2)

P1- Critical, P2- Recommended, P3- Best Practice

To be available at: https://nabanet.com/cybersecuritysubcommittee/

NABA Cybersecurity Recommendations – 2021+

- Content Security and Protection, i.e. “Deepfakes” (P1)
- All-IP (SMPTE ST-2110) Production Facility Lessons Learned (P1)
- Assessment of Third Party/Vendor Security (P2)
- Best Practices in Authentication (P2)
- Recommended Enterprise Investment in Cybersecurity (P2)
- Benchmarking NABA Members’ Cybersecurity Maturity (P3)

P1- Critical, P2- Recommended, P3- Best Practice

EBU and Cybersecurity

EBU
OPERATING EUROVISION AND EURORADIO

- EBU has a well-established Cybersecurity Committee and has developed numerous Recommendations, all available at www.ebu.ch:
  - R141 – Mitigation of Distributed Denial-of-Service (DDoS) Attacks
  - R142 – Cybersecurity of Connected TV's
  - R143 – Cybersecurity for Media Vendor Systems, Software and Services
  - R144 – Cybersecurity Governance for Media Companies

Cont'd

EBU and Cybersecurity (cont'd)

EBU

OPERATING EUROVISION AND EURORADIO

- R145 – Mitigating Ransomware and Malware Attacks
- R146 – Cloud Security, including Procurement, Architecture and Cloud Service Provider Assessment
- R148 – Networked Media Equipment
- R160 & R161 – Vulnerability Management, including inside the JT-NM Program

- Available for free at www.ebu.ch

World Broadcasting Unions (WBU)

- African Union of Broadcasting (AUB)
- Arab States Broadcasting Union (ASBU)
- Asia-Pacific Broadcasting Union (ABU)
- Caribbean Broadcasting Union (CBU)
- European Broadcasting Union (EBU)
- International Association of Broadcasting (IAB/AIR)
- North American Broadcasters Association (NABA)

WBU Technical Committee

- **Chairman**:
  - John Lee, Chairman, NABA Technical Committee
- **Vice-Chairmen:**
  - Antonio Arcidiacono, Director of Technology and Innovation, EBU
  - Bassil Zoubi, Technical Director, ASBU
- **Membership:**
  - All Broadcasting Unions
- **Next Meeting:**
  - December 14, 2020

First WBU Cybersecurity Recommendation

World Broadcasting Unions

- Combined EBU, NABA, ABU and other Union input to produce “WBU Cyber Security Recommendations for Media Vendors’ Systems, Software and Services”, released in January 2018
  - Recommendations to industry, not requirements
  - To be included in RFI’s, RFP’s and RFQ’s to industry to ascertain a potential supplier’s or product’s level of cyber maturity
  - Free-of-charge “living” document, to be reviewed and updated regularly by the WBU

First WBU Cybersecurity Recommendation (cont'd)

- 34 recommendations in total
- Identifies priorities of recommendations: P1 (critical), P2 (important), P3 (best practice)
- Recommendations address: Communications, Authentication, Controls, Documentation, Encryption and Network Configuration
- Available at: https://worldbroadcastingunions.org/

Second WBU Recommendation: Core Cybersecurity Controls or Basic Cyber Hygiene

- Approved by the WBU in October 2018
- **Undertaking these steps can prevent up to 70% of cyber attacks**

Second WBU Recommendation: Core Cybersecurity Controls or Basic Cyber Hygiene

- Actively inventory and track all devices on the network
- Prohibit the installation of all software unless it follows an approved change control process
- Establish secure configurations for hardware and software on mobile devices, laptops, workstations and servers

Second WBU Recommendation: Core Cybersecurity Controls or Basic Cyber Hygiene (cont'd)

- Continuously run vulnerability assessments and remediation
- Minimize administrative privileges and regularly assess whether those who have administrative accounts require them, on an on-going basis.
- Institute regular, on-going cyber security training of all staff

Available at https://nabanet.com/cybersecuritysubcommittee/

Third WBU Recommendation: Cloud Security

- EBU has already issued very detailed recommendations, namely R146, “Cloud Security for Media Companies”
- NABA has issued two cloud-related recommendations, one on SaaS and a second on private cloud
- Cloud Security recommendation was approved in 2020

Third WBU Recommendation: Cloud Security

World Broadcasting Unions

- Cloud security is a shared responsibility between the cloud service provider and the broadcaster - the demarcation point should be clearly defined;
- Broadcasters should undertake a priority classification of data to be transferred - overly sensitive or mission critical material should be retained in the enterprise and not transferred to the public cloud;
- Comprehensive internal enterprise access controls should be replicated in the cloud, multiple processes regarding access and identity management should be avoided;

Third WBU Recommendation: Cloud Security (cont’d)

- The use of virtual private cloud is preferred to multi-tenant public cloud as it provides integrated control and threat assessment for the broadcaster;
- Continuous and stringent vulnerability assessments must be undertaken by the cloud service provider to minimize both service provider and broadcasters’ vulnerabilities;

Third WBU Recommendation: Cloud Security (cont'd)

World Broadcasting Unions

- Data encryption in the cloud is crucial for robust cybersecurity, including when such data is in motion or at rest. This is particularly important when importing or exporting data;
- Broadcasters should implement comprehensive Intrusion Detection Systems (IDS) when implementing any cloud solution, to identify unauthorized data ingress or egress;
- Data deletion policies and associated processes should be documented between the parties before migrating to the cloud;

Third WBU Recommendation: Cloud Security (cont'd)

World Broadcasting Unions

- As part of the broadcaster's overall enterprise security program, continually train broadcasters' employees on cloud security, including the detection and mitigation of malicious or suspicious activity in the cloud environment;
- Regularly conduct security audits, including third-party audits, of all broadcasters' systems, including all cloud infrastructure, in order to identify and mitigate vulnerabilities and security gaps.

Cyber Threats to the Media/ Broadcasting Industries

- Industry is now quickly adopting:
  - IP-based technology to support the bandwidths and speeds of next generation television systems
  - Cloud services for financial or agility reasons
  - Multi-protocol delivery of content over IP networks to a wide range of consumer devices
  - OTT or broadband services for direct consumer delivery of digital content
- These may broaden the threat “surface” and make broadcasters more vulnerable to attack.

Cybersecurity in the Media/ Broadcast Enterprise

- Maintain cyber security as a Board of Directors’ and C-suite priority due to the risk to the enterprise
- Strengthen cyber security program throughout the enterprise, including on-going governance and risk assessment
- Proactively implement behavioural change in staff, not merely train
- Invest annually in cybersecurity including a dedicated cybersecurity team
  - 10% to 15% of overall IT spend, depending on aversion to risk

Broadcasters, Media Vendors and Cyber Security

- EBU, NABA, the WBU and other Unions have issued recommendations and look for feedback on these positions
- Broadcasters and their vendors/service providers should engage on the cyber maturity of the products and services broadcasters use
- Vendors can consider joining in to these discussions to have their voice heard in cybersecurity discussions

Conclusions

- Broadcasters are adopting IP technologies, like SMPTE's ST-2110 family of standards, JT-NM-1001-1, IPMX
  - May broaden the threat surface for cyber attacks
- WBU cybersecurity recommendations have been issued
  - Media Vendors' System, Software and Services
  - Core Cyber Security Controls
  - Cloud Security
- Broadcasting Unions, like NABA, the EBU and the ABU, are engaged and working diligently on cybersecurity
  - NABA is producing recommendations and has a full workplan for 2020 and beyond

Thank You

John C. Lee, P. Eng.
Chairman, NABA Technical Committee
Chairman, WBU Technical Committee
johnclee464@gmail.com

NABA
NORTH
AMERICAN
BROADCASTERS
ASSOCIATION