• ABU

ASIA-PACIFIC BROADCASTING UNION
- Kuala Lumpur, Malaysia

• ASBU

ARAB STATES BROADCASTING UNION
- Tunis, Tunisia

• AUB

AFRICAN UNION OF BROADCASTING
 - Dakar, Senegal

• CBU

CARIBBEAN BROADCASTING UNION
- St. Michael, Barbados

• EBU

EUROPEAN BROADCASTING UNION
- Geneva, Switzerland

• IAB

INTERNATIONAL ASSOCIATION OF
BROADCASTING
- Montevideo, Uruguay

• NABA

NORTH AMERICAN
 BROADCASTERS ASSOCIATION
 - Toronto, Canada

WBU-TC Recommendations for Core Cyber Security Controls

Several Broadcasting Unions have been active recently in the realm of Information Security, specifically Cyber Security. The World Broadcasting Unions Technical Committee is recommending a minimal set of controls that all broadcasters can take to provide a base level of protection against cyber attack.

These top six controls[1] are:

- Actively inventory and track all devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
- Prohibit the installation of all software unless it follows an approved change control process. This applies to all servers, workstations, and laptops.
- Establish secure configurations for hardware and software on mobile devices, laptops, workstations and servers, including the timely application of software patches.
- Continuously run vulnerability assessments and remediation, via the use of automated scanning tools on all systems and users on the network.
- Minimize administrative privileges, only use administrative accounts when they are required 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 employees in the enterprise, specifically focussed on detecting phishing attacks and other related exploits.

WBU-TC
October 3, 2018

---

1 These recommendations are in line with the Center for Internet Security (CIS)'s top controls. https://www.cisecurity.org/