Digital Alert Systems

Industry Advisory

Understanding Security for Your EAS Equipment

Best Practices and Recommendations for Users

Because the Emergency Alert System (EAS) equipment is required to be connected to the Internet, broadcasters have been introduced to all manner of security risks. However, these risks exist for any key system a broadcaster may have connected to an untrusted external network like the Internet.

EAS devices are no longer isolated in the broadcasters' operation – they are connected externally to monitor government sources of alert data, and are increasingly connected internally to interface with other broadcast systems. This is no different from many other key assets in a broadcast operation. Connections to the outside world create security risks. Security risks can come with a high price for broadcasters. However, many of these risks can be lessened with simple, straightforward steps to protect your networks, critical equipment, and company information.

On the other hand, attacks and breaches of your systems – including your EAS equipment – can cost time and money – including the disruption of regular business activities, costs to identify and correct the problem, or even the costs to the image and integrity of the broadcasters' image. Taking a few steps to proactively improve your cybersecurity can save a broadcaster innumerable complications and costs. Commonsense steps to improve security can help protect critical broadcast infrastructure, business information, the integrity of the broadcast operation, and the integrity of the Emergency Alert System itself.

Correcting poor security practices can help protect critical broadcast assets, minimize risk, reduce exposure and potentially lower costs.

Better awareness of the security issues, and the means to address them, can help protect the integrity and reputation of broadcasters and the Emergency Alert System.

EAS equipment is generally not designed as standalone security devices. Simply stated, this equipment should never be exposed directly to the public Internet. Nor should any other key equipment in your broadcast operations be directly exposed to the Internet. This equipment must be utilized in conjunction with other network, physical and operational security measures.

Digital Alert Systems
A division of Monroe Electronics
585-765-1155 | fax 585-765-9330
100 Housel Ave. | Lyndonville | NY | 14098
www.digitalalertsystems.com

15 January 2014   Revision 1.0

The maintenance of EAS equipment presents a special role and responsibility, unlike many IT systems and devices. When properly used, the Emergency Alert System presents the opportunity to help safeguard the lives and property of citizens. On the other hand, if misused, attacked or exploited, the EAS could risk the safety of the public it was designed to protec.

For this reason, Digital Alert Systems has worked to present users of EAS devices with simple, commonsense cybersecurity best practices, to help guide both users in securing and protecting their EAS devices.

EAS Security Best Practices and Recommendations

Fortunately, security controls for EAS are by and large no different than security controls in any IT environment. This includes your facility, network infrastructure and IT systems, and even the people that have access to this key equipment.

We have developed a list of EAS Security Best Practices for Broadcasters, which provide a basic framework for broadcasters to assess their own respective cybersecurity readiness, to hopefully make informed decisions on areas of potential improvement.

These recommended best practices are built upon a growing body of knowledge that is available in multiple industry sectors, including numerous best practices generated by the Network Reliability and Interoperability Council (NRIC) and its successor, the FCC's Communications Security, Reliability and Interoperability Council (CSRIC). References and a directory of resources are provided at the end of this document.

Recommended EAS Security Best Practices for Broadcasters

Issue	Best Practice Recommendation
Make security part of your business plan	Broadcasters (EAS device users) should include security as an integral part of the strategic business planning and decision making process to ensure that security risks are properly identified and appropriately mitigated.
Create Corporate Security Policies	Broadcasters should establish and implement corporate security standards and requirements in consideration of the best practices of the general communications industry (e.g., published best practices from DHS, FCC, CSRIC, NRIC and others).
Check your IT networks and equipment.	Broadcasters, in consideration of FCC rules, should develop and implement periodic physical inspections and maintenance as required for all critical systems, including EAS Equipment.
Keep your EAS gear physically secure.	Broadcasters should ALWAYS maintain EAS Equipment in a secure PHYSICAL environment. Access controls may include limitations on the ability for unauthorized individuals to access the equipment, and other measures.
Keep your EAS gear in a secure network.	Broadcasters should ALWAYS maintain EAS Equipment in a secure NETWORK environment. Because this equipment has been designated by the FCC to be Internet facing, basic network security protocols must be followed at a minimum.

Always Use Firewalls	Broadcasters should ALWAYS maintain a firewall between EAS Equipment and insecure public facing networks (the Internet).
Consider Segmenting Your Networks	Broadcasters may wish to consider segmenting the EAS device (with devices such as firewalls) from both the Internet and the Broadcasters' own intranet and the Internet. In other words, treat the EAS device as a domain in and of itself. Treat each domain as hostile to all other domains. Follow industry recommended firewall policies for protecting critical internal assets.
Disable Unnecessary Services	Broadcasters should identify disable unneeded network accessible services, or provide for additional compensating controls, such as proxy servers, firewalls, or router filter lists, if such services are required.
Configure and use EAS device privilege levels	Where EAS devices provide for different level of privileges for users, Broadcasters should designate "least-privilege" access for each EAS device user to accomplish required tasks using role-based access controls where possible.
Regularly Seek and Install Software Updates and Patches	Broadcasters should establish and implement procedures to (1) periodically check with EAS manufacturers for patches and updates; and (2) ensure that all security patches and updates relevant to the EAS device are promptly applied. If required, the system should be rebooted immediately after patching for the patch to take effect.
Expedite Security Patching	Broadcasters should have processes and tools in place to quickly patch critical infrastructure systems when important updates and security patches are made available by the EAS Manufacturer. Such processes should include determination of when expedited patching is appropriate and identifying the organizational authority to proceed with expedited patching. If possible, this should include expedited lab testing of the patches and their effect on network and component devices.
Apply General System Updates	As appropriate, Broadcasters should deploy security and reliability related software updates (e.g., patches, maintenance releases, dot releases) when available between major software releases. Prior to deployment, appropriate testing should be conducted to ensure that such software updates are ready for deployment in live networks. Equipment Suppliers should include such software updates in the next generic release and relevant previous releases.
Verify Patches Have Been Successfully Applied	Broadcasters should perform a verification process to ensure that patches/fixes are actually applied to EAS devices.
Limit or Restrict Remote Access to your EAS Equipment	Whenever possible, remote access to EAS devices should be severely restricted. Remote access should always be made via a secure pathway, such as VPN. Remote access should NEVER be made possible by an EAS device that is not secured by a firewall, or other network security means.
Harden EAS Device Access Control	Broadcasters should ALWAYS harden the access control capabilities of each EAS device or network element BEFORE deployment to the extent possible (typical steps are to remove default accounts, remove unnecessary accounts, change default passwords, turn on checks for password complexity, turn on password aging, turn on limits on failed password attempts, turn on session inactivity timers, etc.).

Threat Awareness	Broadcasters should monitor EAS Manufacturer information resources to obtain vendor patch/security notifications and services to remain current with new vulnerabilities, viruses, and other security flaws relevant to systems deployed on the network. Broadcasters should ALWAYS make sure the EAS Manufacturer has current and accurate contact information for the Broadcaster.
Use Strong Passwords	Broadcasters should ensure that passwords are sufficiently long and complex to defy brute force guessing and deter password cracking. To assure compliance, perform regular audits of passwords on at least a sampling of the systems. Poorly chosen passwords can easily be guessed by humans or computer algorithms to gain unauthorized access. Examples of poor password practices include: (1) Passwords that are short, simple (e.g., all lower-case letters), or otherwise do not meet typical strength requirements (password strength may depend on the particular EAS device's capability to handle more stringent passwords, (2) passwords that are left as the default vendor supplied value AND (3) passwords that are not changed on a specified interval.
Change Passwords on a Periodic Basis	Broadcasters should implement a policy which considers how often passwords should be changed. Perform regular audits on passwords, including privileged passwords, on system and network devices. If available, activate features which force password changes.
Prevent Password Disclosure	Passwords should be kept confidential to prevent unauthorized access. Do not post passwords in plain sight, local to a system. Do not share passwords to individual user accounts with associates. Do not send passwords that are not encrypted through unprotected communications.
Always Change Default Passwords	EAS Devices, like many IT products, may be shipped with one or more default passwords. ALWAYS make sure that default passwords have been changed before deployment. Verify that all default passwords (for example administrator and user accounts) have been changed.
Establish "Least Access" User Restrictions	Poorly specified access controls can result in giving an EAS Device user too many or too few privileges. Depending on the capabilities of the EAS device, provide the user with the appropriate level of device and system access (e.g. administrator account vs. user account).
Establish Corporate Security Policy and Awareness Training	Broadcaster senior management should actively support compliance with established corporate security policies and procedures. Broadcasters should provide awareness training to staff that stresses the impact of a security incident, the risks of various levels of threatening conditions and the roles components play in the overall architecture. Training should be provided for personnel involved in the direct operation, maintenance, provisioning, security and support of EAS Equipment.
Removal of Access Privileges	Broadcasters should have policies on changes to and removal of access privileges to EAS equipment and other key systems upon staff member status changes such as terminations, exits, and transfers.

General Cybersecurity Awareness / Safe Computing	Broadcasters should, to the extent possible, ensure their staff is aware of the importance of practicing "safe computing". Broadcasters should protect end user devices and networks from unauthorized access through various methods, including, but not limited to: • Use anti-virus, anti-malware, anti-spyware software in the general computing environment; • Ensure that any software downloads or purchases are from a legitimate source; use firewalls; • Use strong passwords; • Never share passwords; • Configure computers to download critical updates to both the operating system and installed applications automatically; • Scan computers regularly for spyware and other potentially unwanted software; • Keep all applications, application plug-ins, and operating system software current and updated and use their security features; • Exercise caution when opening e-mail attachments; and • Be cautious when downloading programs and viewing Web pages.
Train Staff on Corporate Security Policies	Broadcasters should ensure staff is given awareness training on security policies, standards, procedures, and general best practices. Awareness training should also cover the threats to the confidentiality, integrity, and availability of data including social engineering. Training as part of new employee orientation should be supplemented with regular "refreshers" to all staff.
Create Incident Reporting Processes	Broadcasters should establish an incident reporting mechanism and investigations program so that security related events are recorded, analyzed, and investigated as appropriate.
Recovering from Unauthorized Access	: When an unauthorized remote access to an EAS device occurs, Broadcasters should consider terminating all current remote access, limiting access to the system console, or other tightened security access methods. Continue recovery by re-establishing new passwords, reloading software, running change detection software, or other methods, continuing quarantine until recovery is validated, as practical.
Post-Incident Actions	After a security incident, as may be possible without disrupting operational recovery, Broadcasters should handle and collect information as part of a computer security investigation in accordance with a set of generally accepted evidence-handling procedures.

Conclusion

Cybersecurity is a critical dialogue, as the nation’s Emergency Alert System and related public warning capabilities increasingly leverage the Internet. A fuller understanding of the risks of poor security practices and taking corrective steps can help protect broadcasters’ critical assets, minimize risk, reduce exposure and potentially lower costs. A better awareness of the security issues, and the means to address them, can help protect the integrity and reputation of both broadcasters and the Emergency Alert System.

By considering these best practices and how they may apply to your EAS equipment – as well as other key systems in your operation – you could benefit by:

- Increasing your own network’s reliability
- Increasing regulatory compliance by reducing risks of EAS device or system disruption
- Eliminating vulnerabilities and downtime costs
- Improving the performance of your critical systems
- Avoiding unnecessary costs associated from reacting to and recovering from a cyber incident.

.

References

CSRIC, Working Group 2A Cyber Security Best Practices Final Report, 2011.
(http://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf)

NRIC Best Practices, Network Reliability and Interoperability Council
(https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm, also see
http://www.atis.org/bestpractices/Search.aspx).

Additional Resources

CAP, EAS AND IPAWS: Introducing a Defense in Depth Security Strategy for Cable and IPTV Operations, September 2011, Monroe Electronics. (http://www.monroe-electronics.com/EAS_pages/pdf/ME-WhitePaper_IndAdvisory_Network_Security_091211.pdf)

CAP, EAS AND IPAWS: Introducing a Defense in Depth Security Strategy for Broadcasters, September 2011, Monroe Electronics / Digital Alert Systems.
(http://www.digitalalertsystems.com/pdf/wpdas-122.pdf)

Control Systems Cyber Security: Defense in Depth Strategies, October 2009, U.S. Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT.
(https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf)

Critical Controls for Effective Cyber Defense, SANS. (http://www.sans.org/critical-security-controls/cag4-1.pdf)

Cyber Security Policy Guidebook, Jennifer L. Bayuk, Jason Healey, et al., Wiley, 2012.
Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies (Premier Reference Source), Junaid Ahmed Zubairi and Athar Mahboob, IGI Global, 2011.

Developing a Framework To Improve Critical Infrastructure Cybersecurity, National Institute of Standards, February 12, 2013.

Enterprise Security for the Executive: Setting the Tone from the Top, Jennifer Bayuk, Praeger Publishing, 2009.

Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper, Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, Tech America, March 8, 2011
(https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf).

NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook, National Institute of Standards. (http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf)

NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013, National Institute of Standards. (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf)

NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013, National Institute of Standards.

Password Security, Protection and Management, US CERT, 2012 (http://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf).