RADIOWORLD

THE INTERNET OF BROADCAST THINGS

Media companies will participate in the explosion of the IoT. But "best practices" are still evolving. How should media professionals practice safe IP? Radio needs a framework to hang its IoT on. A practical guide to using and securing IP.

Sponsored by

COMREX BROADCAST RELIABLE

TA THE TELOS ALLIANCE® Create. Communicate. Connect.

INOVONICS BROADCAST Better Radio Since 1972

nautel

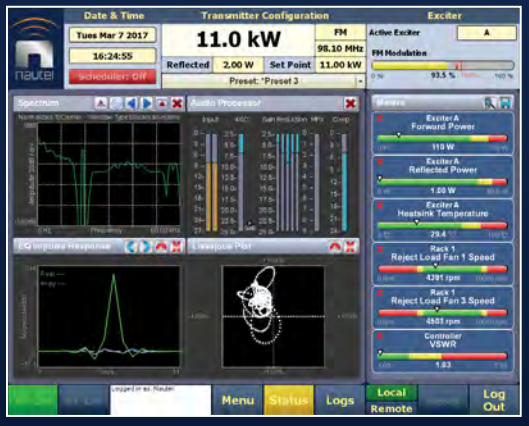
EN ENCO

March 2017

From the Publishers of Radio World

NewBay

PUTTING IP CONNECTIVITY TO WORK



MONITORING AND CONTROL

Over 7,000 transmitters have shipped supporting Nautel's award-winning Advanced User Interface (AUI); a common, easy-to-use interface across all AM/FM transmitters. This innovative, built-in, commercial-grade instrumentation with metering and diagnostics, gives full monitoring and control via touch screen and/or optional web access, helping broadcast engineers save trips, time and money. Learn more ›

PLAYLISTS AND AUTOMATION

Using Nautel's AUI, you can set-up basic automation capabilities, send new content as audio files, and send updated playlists to the transmitter, which then plays the content locally.

BACKUP AUDIO AUTOMATION

Nautel transmitters accept a broad variety of IP, digital/analog inputs giving you the opportunity to define automatic fail-over modes should an input be disrupted. Playlists can be configured to play from a connected USB device.

Livewire

AXIA LIVEWIRE™ IP AUDIO SUPPORT

Broadcasters can connect their Axia Livewire networks directly to a Nautel transmitter to achieve an all-digital transmission path from studio to transmitter without intermediary connections or D/A conversions.

NULLSOFT SHOUTcast

STREAMING INPUT OPTIONS

Streaming support opens up many new possibilities for broadcasters including the option to stay on-air by transmitting the stations SHOUTcast™ stream in the event of a failed STL.

nautel.com

nautel

Cover Art Credit: iStockPhoto.com/jamesteohart

The Internet of Broadcast Things

A practical guide to using and securing IP

Paul McLane
Editor in Chief

IP connectivity is beneficial to broadcasters in so many ways, creating more powerful networks, improving control, allowing remote troubleshooting and so much more.

But "best practices" are still evolving. How should media professionals practice safe IP? We wondered what kind of questions need to be asked as radio contemplates what could be called the growing Internet of Broadcast Things.

What role do firewalls, virtual private networks, password policies etc. play? How can we learn from expert engineers in their work? How are manufacturers responding to the need for more information about responsible IP management? What recommendations are put forth by organizations like the Department of Homeland Security, the FCC and the NAB?

Our sources include Wayne Pecena, assistant director of educational broadcast services at Texas A&M University and a widely respected public speaker on IP networks in broadcasting. We heard some very practical advice from Randy Woods, technical director for the Central Florida Educational Foundation.

Abdul Hakim of the Digital Production Partnership told us that companies should approach cybersecurity issues like they do workplace health and safety training.

In the article "A Framework to Hang Your IoT on," we give you a peek inside a report from an FCC advisory group about what broadcasters can and should be doing. Kelly Williams at NAB pointed us to excellent English-language resources to help translate that report for non-techies.

Josh Thurston, a security strategist in the office of the CTO of Intel Security/McAfee, reflected on what considerations matter most in this discussion. And Kevin Rodgers of our sponsor Nautel talked about how the company's PhoneHome offering fits into this discussion.

My thanks to Radio World contributor Tom Vernon for his participation in this project.

This is Radio World's 30th eBook. When we began our series in 2012 we hardly imagined how popular they'd become. Thank you for reading. Please let us know how we can make the series more useful to you.

Cybersecurity Training Should Be Mandatory

Q
A

Abdul Hakim says treat it like workplace health and safety training

As senior project manager at the Digital Production Partnership, Abdul Hakim has 13 years' experience in the broadcasting and IT industry; he has a comprehensive background in project management and operations at the BBC as well as in the commercial sector.

Q: *Are media organizations a bigger target today for cyber criminals?*
A: Two or three years ago, cybersecurity was a non-issue for most media groups. But now it's become a standing item at board meetings and at the top of corporate risk registers. It's also an area to which a lot of time, attention and resources are assigned.

Cyber attacks on media companies are nothing new, but the turning point seems to be around 2008, with an increase in both the number and severity of attacks. In 2011 Sony was hacked, and reportedly details of a million user accounts were stolen from its Playstation network. More recently details of data loss have emerged for many high-profile companies such as Carphone Warehouse, TalkTalk, Yahoo, LinkedIn, with details of several million accounts stolen.

Furthermore, the current global climate has made media companies an attractive target for hostile groups, who see the disruption of broadcast operations as a major opportunity to gain exposure. A high-profile example was the attack on TV5 in France.

Q: *Do you have any numbers on percentages of cyber attacks, or percentage increase in recent years?*
A: According to the PwC Global State of Information Security Survey 2017 report, the Entertainment, Media and Communications companies surveyed reported an overall increase since 2014, reaching 7,674 incidents in 2016. The total financial losses as a result of these incidents soared by 81 percent in 2016.

Q: *What are some of the top tips to protect yourself or your organization from hacks and cybercriminals?*
A: Making cybersecurity someone's responsibility is a crucial step to take if an organization is to protect itself from hackers and cyber criminals. That person needs to be senior and afforded the budget to be able to tackle any gaps in defenses. They need to have the mandate to make the necessary changes to make sure the organization is protected.

Secondly, it's widely acknowledged that you can have the best defense in the world, with state-of-the-art firewalls and virus/malware scanning tools, but the weakest link in the chain is people. It's still all too common for people to choose obvious passwords, or not to change passwords at all, and for people to download random software, games and other content from compromised or malicious websites. Training and awareness are therefore hugely important. Cybersecurity training needs to become mandatory, just like workplace health and safety training.

Q: *What sorts of precautions do you need to take when traveling abroad with encrypted devices?*
A: In some countries, local laws prohibit you from taking in encrypted devices, while in others, export laws prohibit you from taking out encrypted devices. It's more about the encryption technology than the device itself. For those countries, you will need to know how to turn off encryption. If you're carrying a production laptop it can take a day or two to fully decrypt, so you will need to allow time for that.

If you're traveling to any hostile territories or countries where state-sponsored cyber hacking is common, it's best to take a fresh device installed with only the software you need. Avoid sending sensitive or confidential information over the Internet as these are heavily monitored by state agencies. ■

Security Is a Lot of Non-Stop Work

Q
A

Wayne Pecena preaches the gospel of appropriate protections

Wayne M. Pecena is assistant director information technology of educational broadcast services at Texas A&M University. He serves as the director of engineering for KAMU Public Radio and Television. He was the 2014 recipient of the Radio World Excellence in Engineering Award.

Q: *Give us the "10,000-foot view" on internet security in the broadcast plant.*

A: Security is an ongoing process that, unfortunately, tends to be treated as a one-time, set-it-up-and-forget-it event. It involves continuous assessment, monitoring and action steps.

Security is a lot of non-stop work. For the broadcast engineer actively engaged in maintaining the station technical plant, network security is the "Permanent Employment Act."

Q: *Generally speaking, what are the key advantages to broadcasters of having internet connectivity? With all the attention to breaches, it might be tempting to just disconnect everything. Instead, how can media professionals do it smart, and practice "safe IP"?*

A: It's really all about capability and flexibility. Having an internet connection provides things such as program origination, simplified device remote control, as well as remote management and equipment diagnostics.

Appropriate protection(s) must be used. The days of the open Internet are long gone. I am a proponent of segmented networks, which provide performance enhancement and are also the platform for multi-level security defense implementation. The VLAN, VPN and a firewall are some key components used to build a secure environment.

A firewall is important, as connections to the outside world are usually necessary. Inside the station, don't overlook protection among isolated internal networks. Having said all that, it is important not to become overly reliant on a firewall and assume that everything is safe just because you have one. Finally, utilize the OSI model as a structured guide, and implement security at layers 1-3 at the minimum.

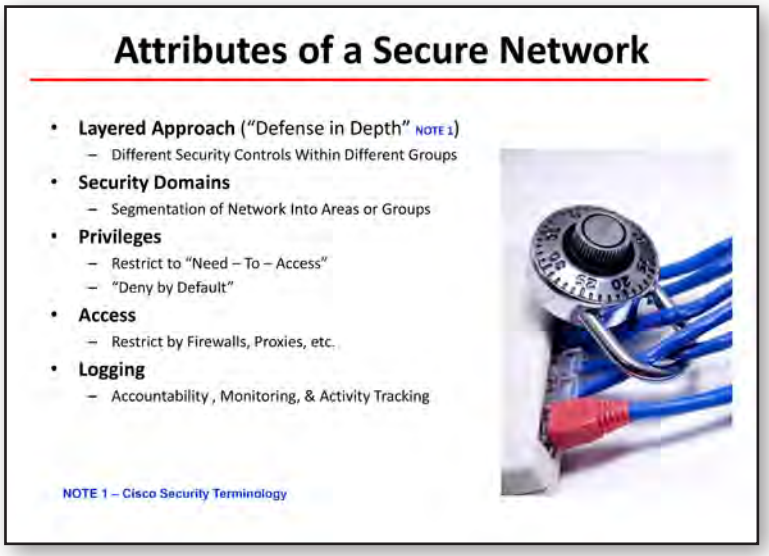


Fig. 1: This image from a Pecena presentation about IP network security identifies attributes of a secure network. Common threats to network infrastructure include DHCP snooping, ARP spoofing/IP spoofing, rogue router advertisements, denial of service attacks and application layer attacks.

Q: *Passwords seem like such a basic concern, but we probably hear about problems there more than any other. What can you recommend to help radio organizations better protect their assets?*

A: Passwords are a surprisingly overlooked issue. The first step is to change default device passwords. This is too commonly overlooked. Then develop your own approach to creating unique and strong passwords. That means something other than your station's call sign, slogan or frequency.

Continued on page **6**

Continued from page 5

A weak password is usually seven characters or less, and consists of dictionary words. Such passwords are dangerous because a hacker can run a script that goes through a dictionary trying words as passwords. And it can do this in fractions of a second. I always recommend passwords that are made up of eight or more characters, containing a mixture of letters and numbers, special characters and upper and lower case. It's also important to avoid using the same password across multiple sites. Otherwise, once a hacker has one password they will have access to all of your accounts.

Q: *Let's talk a bit more in depth. Can you share some important highlights from your presentations about this topic?*

A: As I said, security is an ongoing IT process and should never be considered a one-time, set-up-and-forget process.

Simple-to-implement best practices towards creating a secure network environment include changing host default logins; disabling unnecessary host services; closing unused host TCP/UDP ports; keeping your system software updated and patched; terminating the use of unsecure protocols like Telnet; and using encrypted communications paths such as VPN. (See Fig. 2.)

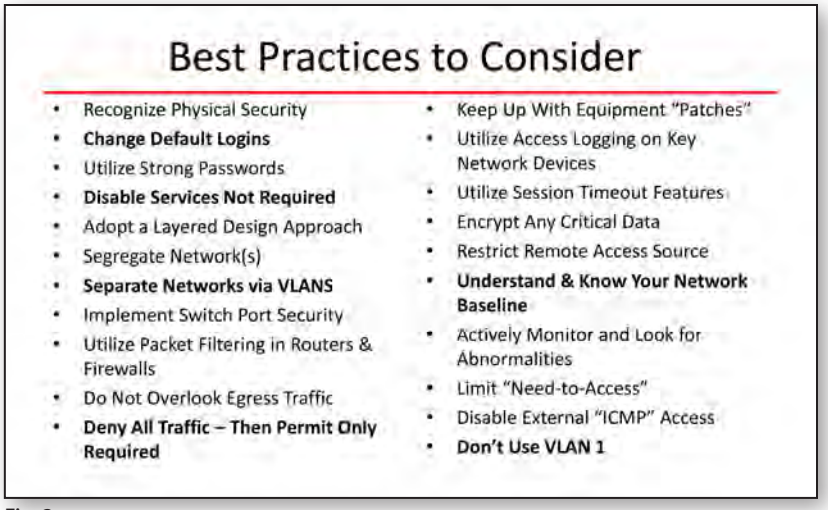


Fig. 2

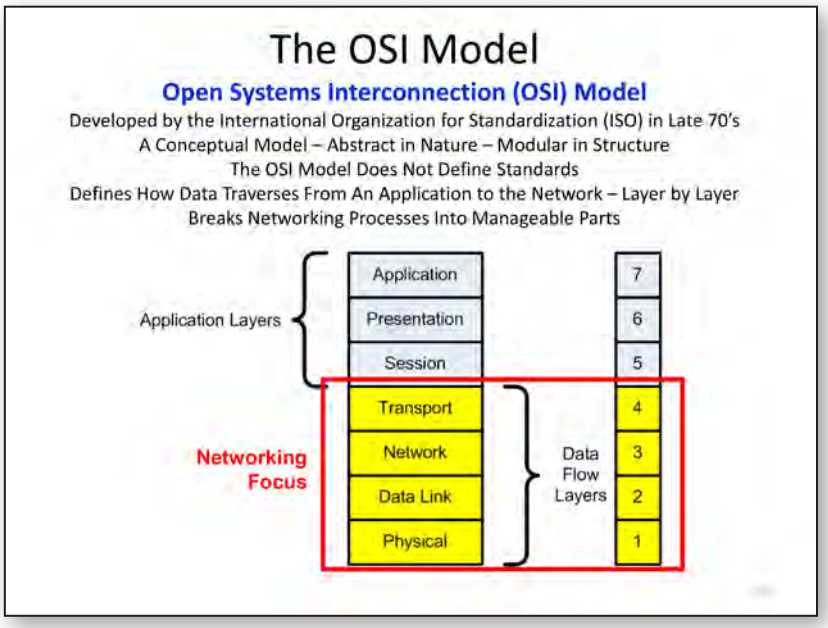


Fig. 3: The Open Systems Interconnection (OSI) Model

Firewalls are an essential tool in the network security toolbox. However, don't over rely on a firewall as the sole protection device. Have more than one "lock" on your door! Deny everything. Open only needed ports. Implement stateless source and destination filtering through an Access Control List (ACL).

Segment networks into protection zones. Minimize the network size/scope. Learn from the "Castle" approach.

Keep in mind that a firewall adds latency. This could impact real-time media found in a broadcast plant. Mitigate by having adequate firewall hardware resources (processor/memory/interfaces).

Q: *What is the Castle approach?*

A: There are several attributes that define a "secure" network. These attributes include utilization of a system design approach that establishes multiple layers of security. There is no single technique to securing a network infrastructure due to the diversity of potential threats.

The Castle approach, also known as "Defense-in-Depth" approach, implements multiple perimeters or layers of security such that if one perimeter is breached another exists to prevent further exploit. Whereas this may be a new approach to network security, it is a centuries-old approach beginning with the design of a castle where the outermost perimeter is protected by a "moat" and additional perimeters must be conquered to reach the core inhabitants or treasures.

A practical implementation approach is to use the OSI Model "Data Flow" layers as a structured guide to network security (Fig. 3).

Start at the Physical layer and limit physical access to network infrastructure hardware and cabling. This can range from electronic access controlled wiring distribution closets to simple lockable rack equipment covers.

Continued on page 8

Comrex Will Introduce ACCESS NX at NAB 2017

Built For The World Of Today

Ten years ago, we developed ACCESS. In those ten years, IP audio transmission technology has continued to grow by leaps and bounds. The state of remote IP infrastructure today is light years removed from the infrastructure of the previous decade.

In response to these trends, we've continued to evolve as well. Our expertise has grown significantly - we've optimized our ACCESS firmware continuously over time, and we're proud of the way ACCESS has grown.

We felt that our beautiful updated software deserved a hardware platform that was built for the world of today, not the world of ten years ago. So we redesigned ACCESS from the ground up, and created ACCESS NX.

ACCESS NX

ACCESS NX features a hardware platform that is optimized for running CrossLock, Comrex's custom reliability layer. CrossLock enables both powerful error correction and network bonding, and intelligently monitors and dynamically adjusts network connections in real-time.

CrossLock™ VPN

ACCESS NX's updated hardware platform improves user experience with faster processors and a five-inch capacitive touch screen that doesn't require a stylus. Other notable hardware features include a new second mic input, phantom power, and an internal battery. ACCESS NX will be compatible with an ACCESS clip-on channel mixer, a new accessory which adds four mic/line inputs and headphone outputs.

Bring your remotes into the future.
Visit us at NAB at Booth# C1633

COMREX
BROADCAST RELIABLE

Write to us at info@comrex.com or call 1-978-784-1776 / 1-800-247-1776

Continued from page 6

At the Data-Link layer, implement managed Ethernet switch security provisions. Control what can be connected to the network by utilizing switch port security. Configure your switch to shutdown port when a violation occurs. Implement VLANs to segment or separate network traffic into security domains. This approach also can improve network performance by limiting a network broadcast domain.

Fig. 4: The Castle or "Defense-in-Depth" approach to network security is based upon a centuries-old concept.

At the Network layer, implement firewall filtering techniques and Layer 3 encryption such as IPSec between critical network devices and/or hosts. Firewall techniques include stateless implementations via Access Control Lists (ACL) as well as statefull implementation at the network border. Implement Ingress and Egress filtering. Deny by default. Be a good network neighbor by implementing egress filtering. Do not overlook internal firewalls.

The Transport layer provides another opportunity to implement encryption. Layer 4 encryption includes techniques such as Secure Sockets Layer (SSL).

And finally, a secure network establishes an "Audit Trail" by tracking and monitoring of network activity. Monitoring of unusual network activity is often an indication that a breach has occurred. Audit trails are the key to determining how a breach occurred and to the development of preventative measures for the future. Logging of denied access attempts gives you an indication of potential threats being imposed on the network.

In summary, a network is considered secure when Defense-in-Depth design techniques are implemented with restricted access via internal and external firewall techniques where all activity is monitored and logged.

Q: *You've also noted that many discussions of IT security focus on protection of servers and desktop workstations but that this might not be sufficient for broadcasters.*

A: Servers and desktops commonly incorporate robust security features based on their native operating system. Think about how many Tuesday Windows updates are security related.

Outside of the administrative offices, the typical broadcast plant has functional devices in the program content stream such as an EAS decoder, maybe a transmission codec, automation systems and a media content storage server. These platforms likely have a common operating system such as Windows or Linux at their core; however these systems are often "stripped down" versions of the operating system or an embedded operating system that often lack the robust operating system security systems.

From a practical standpoint, can I execute a common antivirus protection program on my EAS encoder/decoder? Likely not!

So the broadcast plant offers additional challenges that must be addressed outside the scope of the broadcast device. Thus, techniques outlined in virtually all of the responses in this eBook point to solutions such as network isolation or segmentation, firewalls with multiple DMZs or security zones, limiting host communications scope to or from the broadcast device, and outright eliminating outside access to the device.

With regards to remote access, I am a champion for an IP-based KVM switch of your favorite brand. I like Raritan. Of course the KVM switch should be accessed via a VPN when offsite.

Wayne Pecena will give the presentation "Is Your Network Really Secure?" at the 2017 NAB Show Broadcast Engineering and Information Technology Conference on Wednesday April 26 at 4:30 p.m. He'll provide an overview of tools to verify and ensure that desired network security provisions are actually in place, with a focus on penetration testing and public domain security tools like Nmap. ■

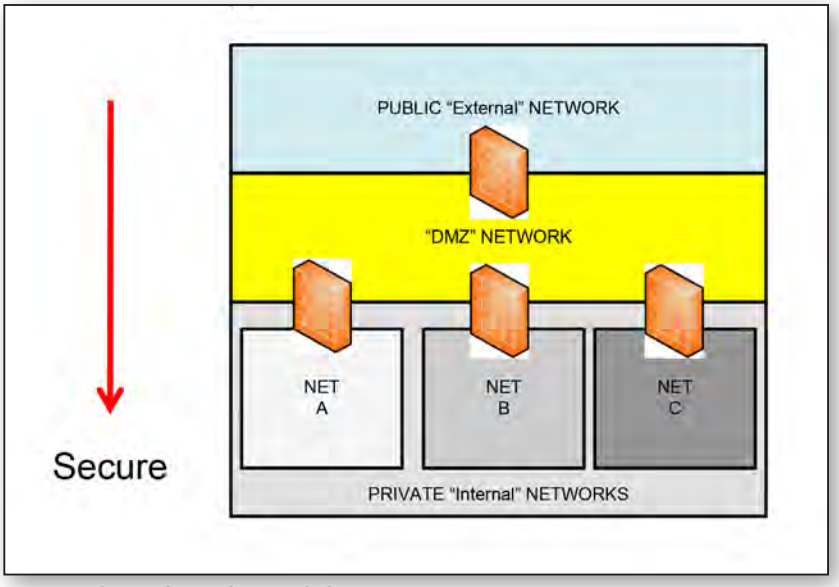


Fig. 5: Applying a layered network design.

PhoneHome Creates Virtual Session in Cloud

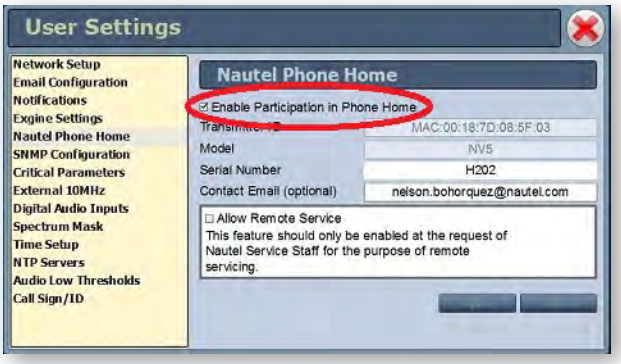
Q
A

Kevin Rodgers says the service makes customer support a proactive endeavor

Kevin Rodgers is president and CEO of Nautel, a manufacturer of radio broadcast transmitters and sponsor of this eBook.

Q: *Tell us a bit about the origins of Nautel's PhoneHome service.*
A: We launched the service in 2013. Our goal was to motivate customers to connect their transmitters to the internet. The biggest restraining force was security issues surrounding a conventional IP connection that gave access to all command and control functions.

Our strategy with PhoneHome was to build a product that sends information rather than receives it. Our transmitters already collect an enormous amount of data. So we proactively send this information to the cloud via the internet. There is no need for customers to grant access through the network's firewall.



An image from the Nautel website shows how to activate PhoneHome in the user settings of the transmitter AUI.

PhoneHome creates a virtual session that takes place in the cloud, making it firewall friendly.

Q: *How has this changed the way you handle tech support?*
A: It changes everything. Customer support has shifted from a reactive to a proactive endeavor.

Our customer service techs can use PhoneHome to analyze data in real time, even accessing the live AUI (Advanced User Interface), or to view the state of a customer's transmitter at any time leading up to a fault. This unique diagnostic approach allows our support staff to travel back in time and review the events leading up to and during an alarm occurrence, giving them valuable insight into how a transmitter is behaving before, during and after an alarm, as well as how this behavior may be related to the alarm event. Before PhoneHome, the techs were usually called after a failure, and had to rely on the recollections of the customer, which might be incomplete or inaccurate.

This proactive support allows us to diagnose problems quickly, overcome language barriers and get customers back on the air faster.

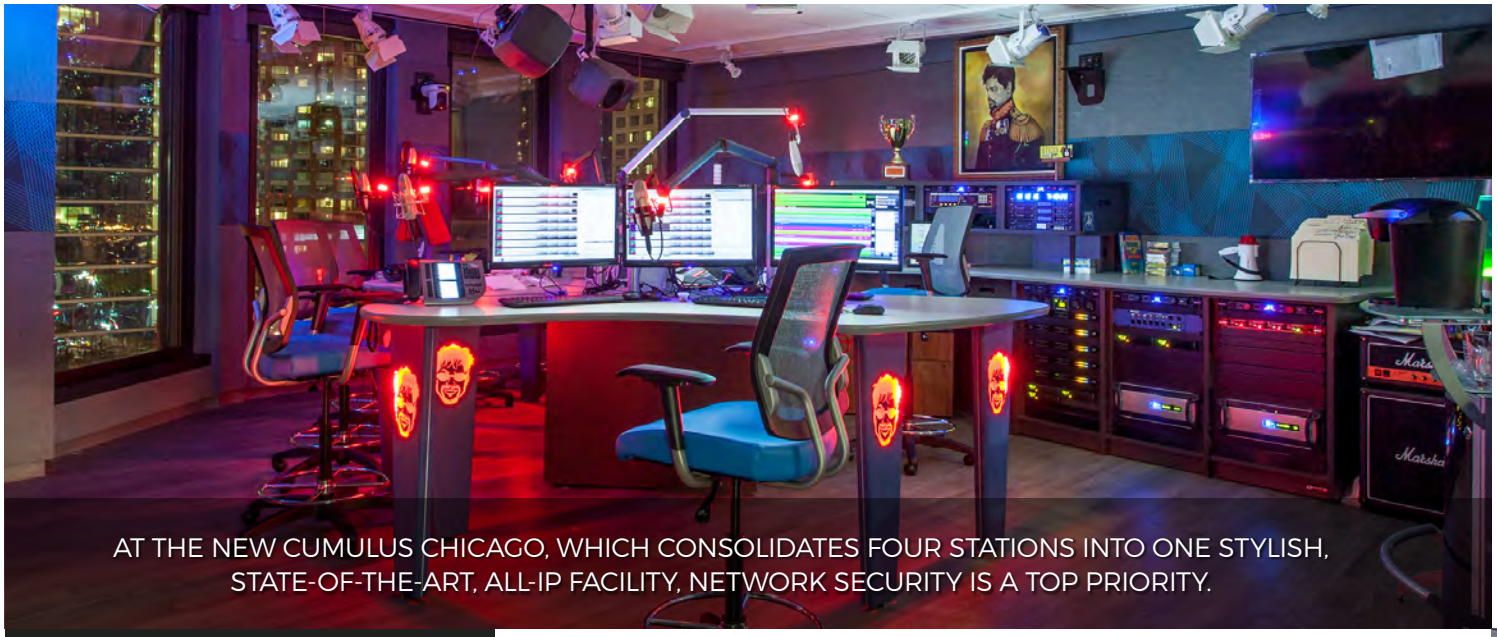
Q: *Participation in the PhoneHome service is voluntary. What sort of response have you had from customers?*
A: We've been very pleased. So far, around 600 customers have signed up. We expect that number continue to increase, both from new sales and also as transmitter sites in extremely rural areas finally get internet access.

Q: *Tell us about one of your success stories with PhoneHome.*
A: As we were scanning the PhoneHome data that comes back to Nautel, we saw one customer had a power module that had failed. Since it was still under warranty, we shipped him a replacement before he asked for it, or even realized that he needed it. ■

Keeping Your Broadcast IP Network

Safe in the Age of IoT

By Greg Shay, CTO, the Telos Alliance



AT THE NEW CUMULUS CHICAGO, WHICH CONSOLIDATES FOUR STATIONS INTO ONE STYLISH, STATE-OF-THE-ART, ALL-IP FACILITY, NETWORK SECURITY IS A TOP PRIORITY.

Considering an Audio over IP (AoIP) network for your facility makes sense; it's faster, cheaper, and better than previous technologies. By converting to AoIP, you not only tap into the power of current technology, you allow your facility to leverage the enormous universe of "off the shelf" IT devices that are used worldwide, and not just in the broadcast industry.

Just like those connected IT devices, IP-based broadcast gear can open up your network to vulnerabilities, which is why it's important to take measures to secure it. Broadcast security has always been a priority. Since the first broadcast cable, there was a pair of wire cutters. The security methods are just different now. Here are some of the most common questions I get asked about network safety, and our advice for keeping your network impenetrable.

HOW DO I KEEP MY BROADCAST IP NETWORK SAFE?

For safe IP, media professionals should use best practices borrowed from the IT industry, and make use of the knowledge, skills, and capabilities of IT professionals and expert contract engineers. In the same way broadcast has borrowed technology from the IT industry, we should also borrow best practices for IT security and reliability.

HOW DO FACILITIES AVOID TENSIONS OVER WHO CONTROLS THE STUDIO, *THE ENGINEER* OR *THE IT PRO*?

IP broadcast audio represents a different type of IP network traffic than many in the IT worlds of banking and web commerce transactions are used to. But the fundamentals of IP networking are the same. Most valuable is a good IT person who is open-minded and curious, who understands that broadcast media is simply a new and interesting capability that the same IT networks have always had. This attitude is the doorway to productive and good practice, rather than operational conflicts. The fact that one can do banking over the internet (the least secure of all networks), is an example of safe IP networking, and IT engineers are making that possible.

A healthy division of labor is for IT to plan, implement, and maintain the reliable network to make the connections. But the media professionals make the interesting shows, the high-quality programming, that the audience wants to hear. Only the audio professional knows if the end result *sounds good*, and what it takes to produce that.

WHAT KIND OF QUESTIONS NEED TO BE ASKED WHEN USING IP AUDIO IN THE GROWING INTERNET OF THINGS?

Is the network secure? Controlling access to the network used for broadcast is the first, best defense. With a completely open and uncontrolled network, it is difficult for the attached devices themselves to make the network behave the way it needs to.

Said another way, the goal of IP networking for broadcast is to use IP network technology to get the broadcasting job done. That's not saying the same thing as broadcasting over unsecured or uncontrolled networks. It is important see this fundamental difference.

Is the broadcast network openly interconnected with the general internet? This should give pause. Some of the power of IP connectivity is the convenience of access (for example the chief engineer, in the middle of the night from home), but access can be enabled through secure methods, not open connections.

WHAT ROLE DO FIREWALLS, VIRTUAL PRIVATE NETWORKS, AND PASSWORD POLICIES PLAY?

These are all accepted best practices for securely enabling connection and access to IP networks. The simple precaution of not leaving default passwords, for example, has long been best practice in the IT industry. And there are a range of other techniques beyond these. We can expect smarter, safer and more capable networks in the future.

To inherit these present and future network advantages, we must leverage IT equipment for broadcast, so that broadcasters don't themselves have to invent and develop signal transportation methods and equipment that essentially do these same jobs.

Having a good IT professional, an even better division of labor, and being vigilant will make your broadcast network safe and secure.

It's All About the Features and Value

Q
A

Josh Thurston reflects on what considerations matter most

Josh Thurston is a security strategist in the office of the CTO of Intel Security/McAfee. He also co-founded a merchant services company that developed a secure mobile credit-card processing solution over digital wireless devices.

Q: *Is some hardware better than others (i.e. VPN routers)? Do you get what you pay for?*
A: Hardware is getting to a point these days where it is as close to a non-factor as it gets. What really comes into scope are the features, scalability and value. A lot of hardware is also essentially going away because companies are moving their infrastructure to the cloud. I have clients that have moved everything short of a physical router running out of their office into the cloud. The remaining hardware is purchased from manufacturers who offer the best value and the best quality. There are reasons why companies like Cisco, Intel, Juniper and others are all leaders in their own categories: They make great hardware.

Q: *Are hardware firewalls superior to software firewalls?*
A: Once again, it is all about the features and the value. There are instances where throughput or port density is greater for a piece of hardware instead of software, but technology improves so fast that I see that becoming a non-issue.

I also take into consideration the outcomes and use cases a security team is looking for. For example, if you have a very static environment where things don't change, hardware may be the way to go. On the other hand, if you are moving to a virtual shop, and you want features such as VMware Vmotion, then software may be better for you. In fact, there are a number of companies that build the same firewall in the physical and virtual space.

If you have a very static environment where things don't change, hardware may be the way to go.

Q: *Sometimes reporters connect their codec or iPhone to a WiFi network, or management access scheduling software from a remote site. These types of actions leave the system vulnerable to "Man in the Middle" attacks. What are some best practices that broadcasters can apply to protect themselves from such attacks?*
A: Two solutions come to mind. First, there are applications for smartphones and tablets for a VPN to encrypt your tunnel. Second, you can use SaaS Proxy from a number of vendors. At McAfee, we offer a hybrid solution for proxy and we can also add in Cloud Access Security Broker (CASB) to monitor the visualization, encryption and protection using Data Loss Prevention. This would be a great way to protect connections and content. The SaaS proxy-gateway option would be my main preference, and the VPN tunnel would be the second option. ■

"Get Ready for the World of the IoT"

For more from Intel Security Group about the implications of the Internet of Things, see our interview in the March 29 issue of Radio World with Gary Davis, chief consumer security evangelist for the company. "We're basically bringing online about a million devices per hour right now," he said, "and one of the challenges we're seeing from a security perspective is that most of those devices are being brought online without any thought about security."

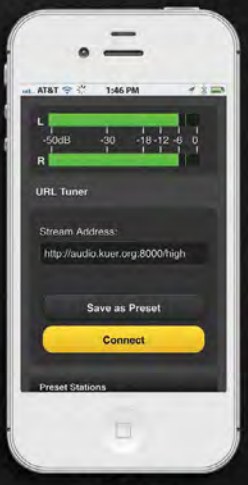
Internet Radio Monitor

610

UNINTERRUPTED MONITORING OF STREAMING ONLINE RADIO

- **Automatically decodes & displays live metadata**
- **Balanced analog L/R & AES-digital outputs**
- **Alarm checks for loss of audio, stream, & Internet**
- **Alerts sent by email and/or text messages**
- **Accurate front-panel LED metering**
- **Responsive Web interface for desktop or mobile**

Desktop



Mobile

Better Radio Since 1972

www.inovonicsbroadcast.com

INOVONICS BROADCAST

Assume That Everyone Is a Criminal

Q
A

Randy Woods says radio engineers need to learn to think like nefarious people

Randy Woods is technical director for the Central Florida Educational Foundation. He recently shared IT secrets in an NAB seminar titled "Quality Engineering on a Tight Budget."

Q: *With all the news about breaches, it must be tempting to just "disconnect everything." How can professionals "do it smart," and practice "safe IP"?*

A: Yes, it's tempting, but we would get so much less done.

From a security standpoint, we need to focus on segmentation and isolation. Depending on what the communications requirements are, this can be accomplished at layer 2 with switches, and VLANs. Another name for this is a de-militarized zone, or DMZ. This isolates traffic, but you still need something to connect that segmented network to the networks that it needs to communicate with, and isolate it from the networks that it doesn't. Using a router, or routing process, you can apply appropriate access control lists (ACLs) to the router interfaces.

If the necessary communication is limited to a known list of IP addresses or networks, this is an easy and acceptable solution. If the communication is from the internet in general, or the device needs to talk to the internet, then deeper packet inspection is preferable, which require a firewall. If you are using some Cisco routers and switches, they have a built-in firewall option called context based access controls, or CBAC for short. This is a cost-effective firewall, but it has limited bandwidth forwarding capability. Various other dedicated firewall options are of course available.

Q: *What kind of questions should engineers and IT managers be asking about the "Internet of Broadcast Things"?*

A: The obvious challenge is to keep the bad guys out of these devices. The less considered aspect is for devices that you are granting third-party access to.

For example, we had an emergency alerting device that we allowed the vendor to connect to, to inject proprietary data into our RDS system, which was then picked up on specialty radio receivers. In this type of situation, you have to assume the worst. You have to assume that the vendor, or bad employee, has a malicious intent, and once they have access to their device, that they might use that device to get to other devices on your network. The best option is to put their devices on an above mentioned DMZ, and to not allow them to connect to anything they do not need to. In my case, they only needed to talk to the RDS encoder, so on their DMZ, I granted no outbound access.

Q: *How do firewalls play into this?*

A: At the internet connection point, firewalls are an absolute minimum requirement. Additional processes such as intrusion detection and/or prevention should also be considered when you are protecting critical data such as personal information from your clients.

Q: *How about virtual private networks?*

A: VPNs come in two general forms: remote access, and point-to-point. Remote access VPNs allow your staff to securely access your private network. A big benefit to using this is that you don't have to open holes in your firewall to allow remote administration. Too often a broadcast engineer will open up a hole to do VNC or remote desktop access. At that point, your network security is as strong as your password and/or your authentication process. In my opinion, this practice should never be done. You are just asking to be breached.

Point-to-point VPNs are great for remote sites that you can only get internet connectivity to. Again, they keep you from having to punch a hole in the firewall at either site.

This brings up another topic: Remote, shared sites. It is not uncommon for a broadcaster to be leasing access in a shared building. If a point-to-point VPN is used, gaining access to your studio facility is as easy as gaining access

to the remote site system, which in many cases is trivial. Make sure you lock down your equipment at these sites. Strong passwords. Locked racks, and secured network ports. On most managed switches, there is a feature called port security. This allows you to lock down the Ethernet ports to specific MAC addresses. If someone gains access to your rack and tries to plug their laptop into your switch, they will not be allowed access.

Q: *What is required to provide outside entities, such as alarm companies and security services, access to a transmitter site network while maintaining security of the network?*
A: Limit their access to a single, static source address. If they cannot provide that, then the answer is no. Then put their devices in a very restrictive DMZ. Only grant access

If a point-to-point VPN is used, gaining access to your studio facility is as easy as gaining access to the remote site system, which in many cases is trivial.

to these devices over the absolutely necessary ports, and never allow them outbound access that they don't need. If their device needs access to the internet, that is not a problem. Just make sure you explicitly deny access to all network address ranges inside your private network first. Then allow them access to the internet. Tell them to use Google's DNS servers, 8.8.8.8, and an outside SMTP server if email is necessary.

Q: *What are the best secure methods for station personnel, such as engineers, to access Ethernet-enabled or controlled equipment at a transmitter site (e.g. secure port forwarding, VNC, etc.)?*
A: The best option is via a private connection such as microwave, or maybe Metro Ethernet. If internet access is the only transport, remote access VPN is the next best option. If that is not possible, consider something like TeamViewer. Make sure your password is solid, and that you don't let it get into the wrong hands.

Q: *If a backup ISP service is employed at a site that is otherwise LAN-connected to the studio, how is that securely integrated into the network?*
A: Just like it would be with a primary internet connection. First start with a managed firewall. If the ISP is only to be used when the LAN connectivity is down, use interior routing protocols to dynamically choose the network's default route. This done by prioritizing the default route coming from the backup ISP firewall lower than the priority of the default route coming from the main ISP device. How to do that technically is outside the scope of this discussion, but is very easy to do in a managed network using Cisco, or similar devices.

Q: *What other questions should we in the industry be asking about this issue?*
A: Out engineering community need to learn how to think like nefarious people. I spoke with a naval commander in the cybersecurity division. Somewhere in that conversation, he said to me, "We love people like you. You build nice, neat, clean networks. Once we get in, we can get to anywhere we want." That was a very offensive statement, but unfortunately, very true. In my past career, I worked to build very robust, high-performing networks and systems. The game has very much changed. We now need to assume that everyone is a criminal, and protect our systems like our reputation depends upon it, because it does.

Q: *Anything else we should know?*
A: Many people assume they have some degree of anonymity because there are so many devices on the Internet. They think someone with malicious intent would need to do a lot of detective work to find their site and devices, but it's really quite easy.

The Shodan.io site is a search engine for the "Internet of Things." By doing a Shodan search for your station's call sign [and] Barix or Burk for example, you can see pages of listings for broadcast devices that are visible on the internet. Information such as IP address, site type, stream mode, connection status and content type is readily available.

You can save yourself a lot of pain by simply changing the default password on these devices to something more robust.

If you're not convinced that there is a crisis at hand, did you know that there are now exploits for network printers? Yes, printer can have agents installed on them to act as a Trojan horse, or to interrogate the print streams and capture confidential information. I am now planning on building a printer DMZ and isolating those seemingly benign devices as well. ■

NAB Embarks on Cybersecurity Evangelism

Q
A

Kelly Williams talks about available resources including the association's education program

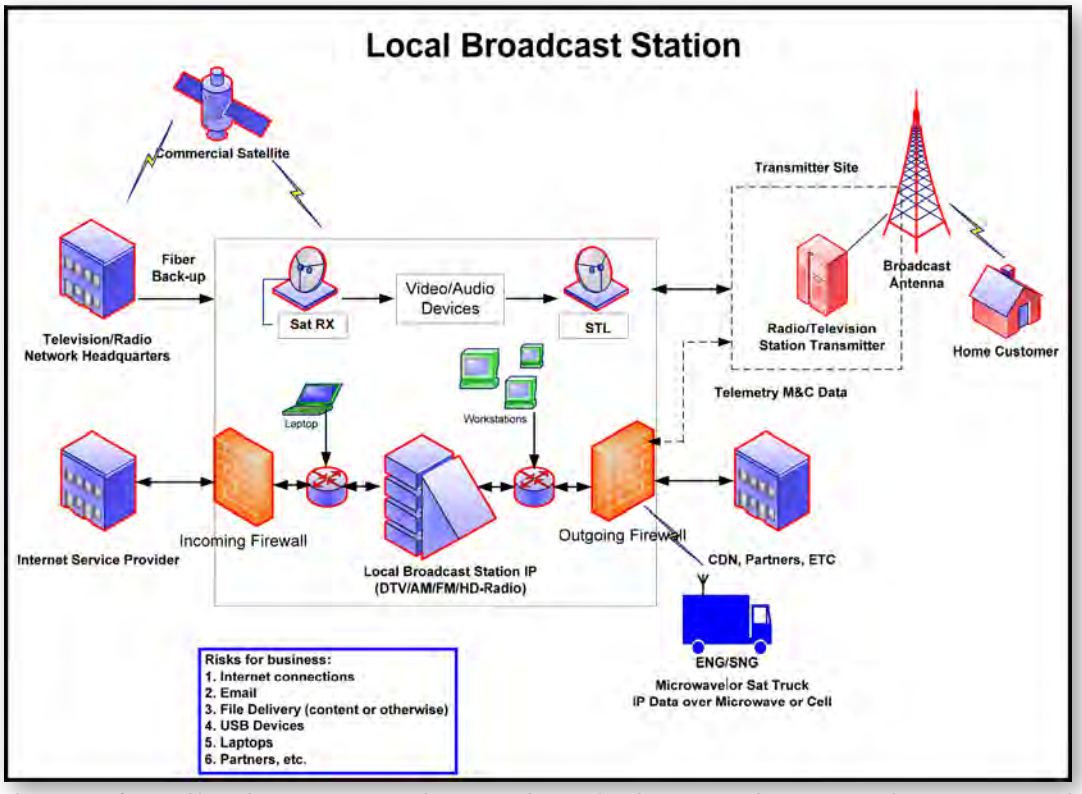
Kelly Williams is senior director, engineering and technology policy in the Technology Department of the National Association of Broadcasters. He joined NAB in 1989 and has worked on technology innovation and has managed a portfolio of technical, regulatory and legislative issues, most recently Next-Gen Television and cybersecurity policy as well as video accessibility, the Emergency Alert System and public alerting. He served on the FCC's CSRIC working group mentioned below.

Q: *What sorts of resources on cybersecurity are available from organizations like the Department of Homeland Security, NIST, FCC and NAB?*

A: There are a number of resources and documents on the Department of Homeland Security's website, although they tend to be more global in scope. The top level for the federal government is the National Institute of Standards and Technology (NIST). They are charged with creating the standards for cybersecurity that all government agencies must adhere to, including the FCC. NIST has a number of reports and papers on its website under the Computer Security Resource Center.

The FCC responded to the NIST mandate by creating CSRIC, the Communications Security Reliability and Interoperability Council. Its mission is to provide

Continued on page **18** ❱



This is one of several broadcast ecosystem architectures depicted in the report "Cybersecurity Risk Management And Best Practices" produced by a working group of the Communications Security Reliability and Interoperability Council.

ENCO

Redefining Radio for the last 25 years.

With over 25 years of innovation, ENCO continues to push the boundaries of what's possible in radio. From advances in remote production and control to virtualization to visual radio technology, ENCO continues to provide stations with the best solutions to reduce overhead, improve workflows and sound better. Contact us now to schedule a personalized demonstration for any of our solutions.

RADIO AUTOMATION • MUSIC SCHEDULING • TRAFFIC
LOGGING • NEWSROOM • VISUAL RADIO • STREAMING
IMAGING • VIRTUALIZATION • CLOUD • DISTRIBUTION

Visit us at NAB Booth N-2024

ENCO

www.ENCO.com/NAB (800) ENCO-SYS fb.com/ENCOsys @ENCOsys

Continued from page 16

recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media and public safety. Its most recent recommendations are on the FCC's CSRIC IV website.

It is important to remember that the federal government considers broadcasters to be part of the critical infrastructure, owing to their ability to keep the public informed in event of emergencies.

For our part, the NAB has embarked on a cybersecurity evangelism and education program. There are two publications on our website, "The Essential Guide to Broadcasting Cybersecurity" and "35 Critical Cyber Security Activities All Broadcasters Should Know" [see sidebar]. The NAB has also created two webinars and two educational courses about cybersecurity. Looking ahead, we are considering creation of a cybersecurity certification program.

Q: *How have strategies to protect organizations from cyber attacks changed over the years?*

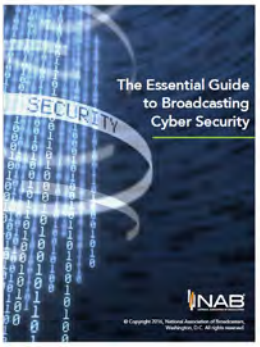
A: It used to be done largely with checklists. When you completed everything on the list, your system could be considered secure. The problem with that was that hackers could use the very same checklists to figure out your soft spots.

NIST has developed a strategy called the Framework, where you determine your risk in five different categories. Your assessment of risk determines the path to security, resulting in a more targeted and unique approach.

Q: *What kind of questions should engineers and IT managers be asking when using IP audio and other IP accessible systems?*

A: There are still a lot of systems out there that run on Windows XP, which hasn't had a security update in three years. Any system in use today needs virus protection, scans and a software firewall. The best systems incorporate Security by Design (SbD), meaning that the system has been designed from the ground up to be secure. Buyers should ask about the operating system of any equipment they are purchasing. Is it the latest version? Is it updated regularly? Can it do virus scans, and does it have a firewall? Has it been built using SbD standards? ■

Check Out These NAB Resources



The NIST publication "Framework for Improving Critical Infrastructure Cybersecurity" provided a broad approach to thinking about cybersecurity as well as practical guidance.

In turn, the FCC's Communications Security, Reliability and Interoperability Council took that framework and offered communications providers, including broadcasters, recommendations based on it.

Seeking to make that information more digestible for stations, the National Association of Broadcasters then published "The Essential Guide to Broadcasting Cybersecurity," picking out the most important broadcast-related recommendations and making them more accessible. And its authors DCT Associates even boiled that down further to "35 Critical Cybersecurity Activities All Broadcasters Should Know." You can download those two files here.

Why go to all this trouble? As the authors put it, "Among many broadcasters the chief desire is for a simple checklist to ensure that newsroom, transmission, remote units and video production operations are sufficiently protected from cyber intrusion and disruption. Because cyber miscreants and threats are constantly evolving, static checklists no longer protect against such things as mutating malware, ransomware, viruses or sophisticated attack campaigns. The NIST Framework and CSRIC recommendations represent a new way of thinking about cybersecurity, offering holistic approaches under which broadcasters can begin to behave differently to ensure continuous, reliable operations."

For more helpful resources, see the NAB's Cybersecurity Resources page.

A Framework to Hang Your IoT on

An NIST outline can help make sense of potential risks for stations going down this road for the first time

Our description of the following document might put you to sleep. But adopting its advice could save you nightmares.

In 2015, a working group of the Communications Security, Reliability and Interoperability Council produced a document called "Cybersecurity Risk Management and Best Practices." Part of it was written by a Broadcast Industry Segment subgroup that developed recommendations to assist in reducing risk to broadcast critical on-air operations by applying a cybersecurity "framework" that had been spelled out by the National Institute for Standards and Technology. Members of this broadcast subgroup came from the National Association of Broadcasters, NPR, Nevada Association of Broadcasters, Monroe Electronics/Digital Alert Systems, CBS Television and the Public Broadcast Service. They encouraged broadcasters to use a "risk management matrix" provided in the document to help with their cybersecurity efforts.

The CSRIC report is well worth reviewing, including the full broadcast section (pages 35–51; find it here). But below is a particularly relevant excerpt from the "Illustrative Use Cases" section of the report.

Cybersecurity involves all broadcast stations regardless of size. As a broadcaster you may think there is no real potential risk to your business from cybersecurity attacks since your business simply puts news and entertainment over the airways.

But, consider how many stations have a web presence and are now streaming the morning news and traffic reports. And that many stations have sophisticated financial system so folks on the road can access everything from the viewer database to sales tools. In engineering, just about everything has an internet connection now (e.g., the EAS system is directly connected to FEMA and National Weather Service for Emergency Alerts).

The NIST Framework can help make sense of potential cybersecurity risks for stations going down this road for the first time. The first step is to take a look at the new cybersecurity framework and make it a part of your business. There are many resources available and technical expertise can be either your internal IT department or an external cybersecurity specialist.

As a local radio or television broadcaster you have a commitment to your community for which you are licensed. Making cybersecurity part of your business protects your revenue, your employees, your viewers, and your community at large. The best way to get started is start small and identify what needs to be protected first.

1) What are you trying to protect?

If you have a news organization there are many systems that are vulnerable for attack. These include but are not limited to: news room computer system, playout servers and automation, graphics machines, news reporters' laptops, and cellular devices used to bring stories in from the field. A firewall is good but cannot protect from bad practices such as not providing controls on network access, unprotected laptops, and "thumb" drives introduced to the network and employees visiting untrusted web sites.

2) Who is responsible/involved in the process?

Cybersecurity isn't someone else's job, it is everyone's job. Support from all stakeholders is the key to success. The support for cybersecurity needs must start at the leadership level and everyone from the General Manager, Programming, News Director, Sales Manager, HR, IT, and Engineering needs to understand and support these efforts.

3) How do you tackle the Framework? What do you do first?

Once the station leaders support the initiative, bring together the stakeholders and provide the guidance and education regarding what is involved and what each individual's roles and responsibilities are. You may find once

Continued on page **20** ❱

Continued from page 19

people are educated there will be better understanding of the process (such as taking systems down to install latest security patches). Cybersecurity can be made to fit any culture.

4) How did you determine what categories and subcategories are the most important? How did you implement the Framework guidance?

Review the framework and focus on what is most important to protect your "critical" systems and work out from there. Businesses can approach the framework in many ways. It doesn't matter if the easy stuff goes first or if the more critical does, but doing nothing is not an option.

5) What are your plans for the future in regard to progressing in maturity?

Once you get through all the initial items on the cybersecurity framework you may find the more you move into to it, the easier it gets. You can then even start on some of the items from the "big guys" to help your continuous improvement process. You may still get groans from the reporters when you make sure their machine is scanned before they can get on the network — but they at least now will know the importance of good cybersecurity.

Proper cybersecurity can work for all businesses and the framework can provide the roadmap.

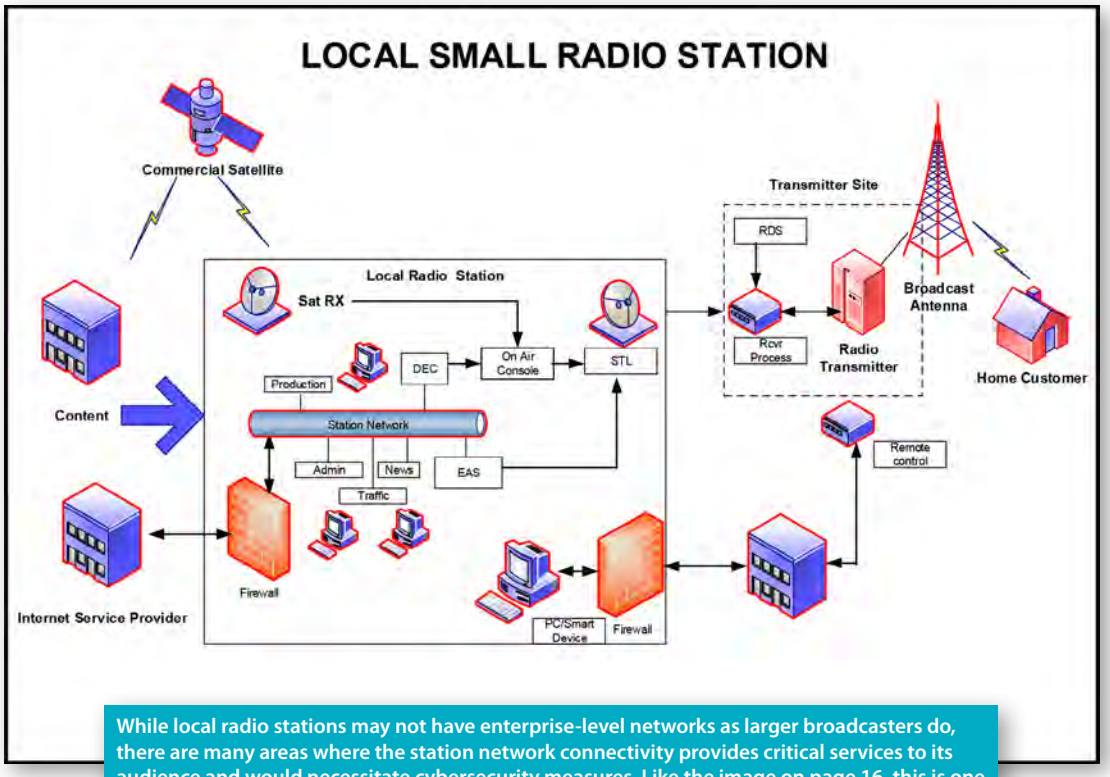
A. Broadcast Radio/TV Station/Hub Assessment

1) Internet Access — In a fast-paced operation where both resources and time are scarce, there is a need to ensure proper security protocols are communicated and followed on a regular basis. In this case, employees are aware of the company's goals and strategy for security, employees are trained and operating procedures and protocols are established and communicated. Examples of this could include use of only "trusted" internet sites, a well-established email policy to ensure employees avoid opening email from "unknown" sources, and discipline in using company and personal resources. This is defined in the analytical framework in several areas:

- Risk Management Strategy
- Awareness and Training
- Communication

2) File/Content Delivery — Broadcasting is moving towards a more IP-based infrastructure where videotape content is being replaced with file based content. These files are large in size and may require special high-speed networks and high-throughput storage systems. Security

Continued on page 22



While local radio stations may not have enterprise-level networks as larger broadcasters do, there are many areas where the station network connectivity provides critical services to its audience and would necessitate cybersecurity measures. Like the image on page 16, this is one of several broadcast ecosystem architectures described in the CSRIC report.

Comrex To Display New Product, Opal, at NAB 2017

Have you ever really looked forward to hearing an interview on a radio program?

Maybe the interview was with a celebrity you admire, or a pundit whose views interest you. Maybe it was with an athlete, or someone at the center of a recent scandal. Regardless of who it was, when it came time for the interview, the guest called in to the studio using a cellphone, and the audio was muddy and difficult to hear. It was hard to understand what they were saying, and so the entire thing felt a little disappointing.

This is why we developed Opal.

Opal makes call-ins sound great. Perfect for coordinating call-ins with guests who have no technical expertise, Opal provides near-studio quality audio with consumer grade equipment. More importantly, connecting with Opal is just as easy as making a phone call - guests don't need to fidget with settings or install apps to connect. All they need to do is click a link.

So what is it?

Opal is short for "Opus Portal" - it's an IP audio gateway. Opal transmits audio using the Opus encoder. Once installed, Opal serves a web page to anyone who accesses it through a browser on a computer or Android device. Once the web page is loaded, the user can click a button and transmit audio from their computer or phone with high fidelity and low delay.

Opal can support two discrete connections at once. Opal occupies 1/2U of rack space, and two can fit side-by-side in a 19" rack shelf. Connections to Opal can only be made from browsers that support WebRTC (Chrome, Firefox and Opal at this time).

opus

Ready to make your call-ins sound great?
Visit us at NAB at Booth# C1633

COMREX
BROADCAST RELIABLE

Write to us at info@comrex.com or call 1-978-784-1776 / 1-800-247-1776

Continued from page 20

measures need to be in place without impeding the timely workflow process required to receive large content files. These files can be delivered through networks, hard drives or even USB type devices. Many of the files are in a proprietary format (e.g., Apple Pro Res, AVID DNX, etc.) and require special security measures. Network delivery systems such as Signiant and Aspera provide the user a path to implement a security layer. This is defined in the analytical framework in the following areas:

- Protective Technology
- Detection Process
- Continuous Monitoring
- Mitigation

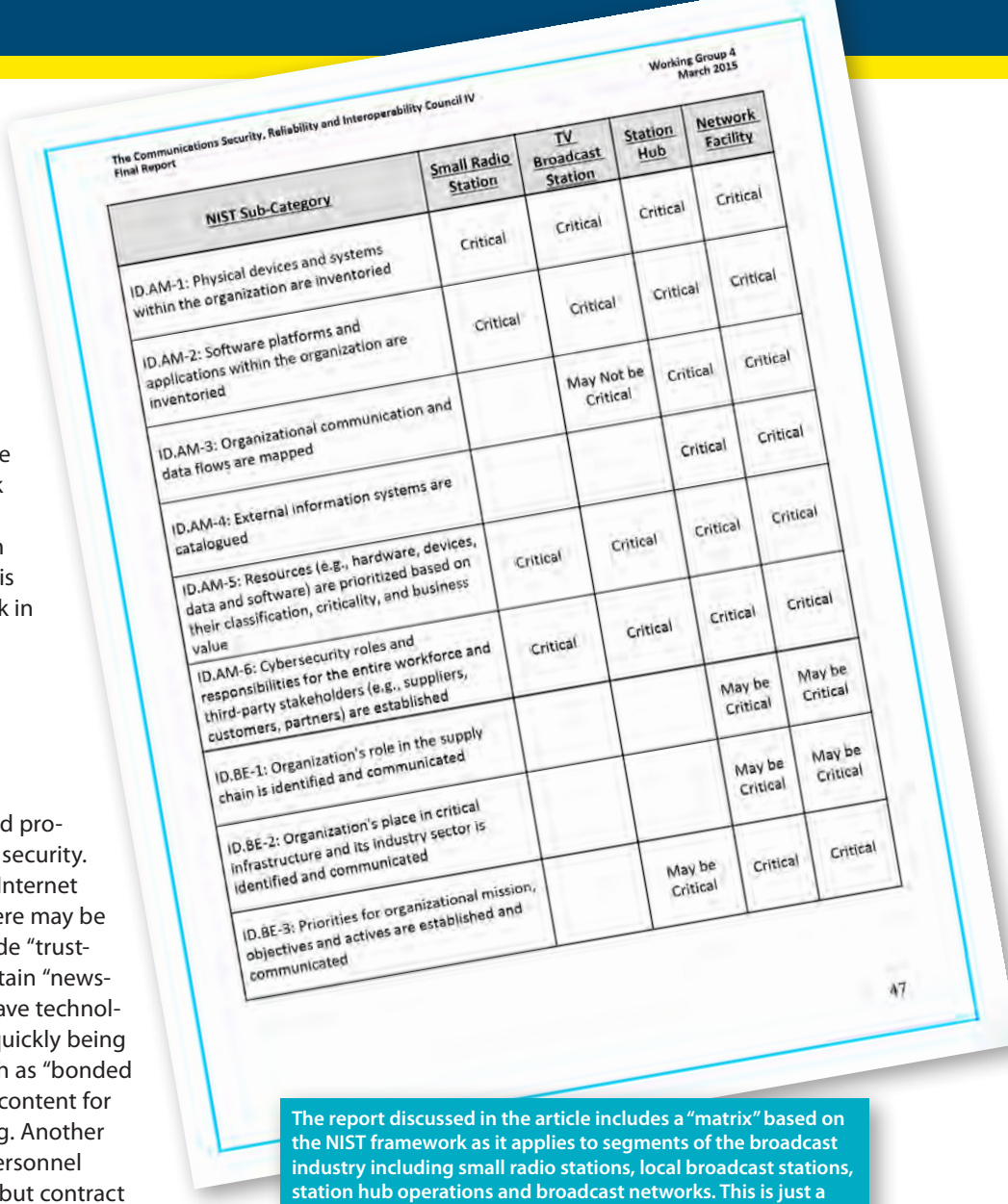
3) News and Production — News and production have unique challenges in security. Many of the policies described in "Internet Access" would be included, but there may be many instances where going outside "trusted" sources may be required to obtain "newsworthy" information. Also, microwave technology for backhaul of "live" shots is quickly being replaced with new technology such as "bonded LTE" to provide "live" or file-based content for news, sports or other programming. Another unique challenge is much of the personnel are often not full-time employees, but contract workers, per diem production staff and "stringers" (such as photographers and camera operators). Providing the proper training and discipline may be difficult and require careful vetting and clear and easy to understand expectations and procedures. This is defined in the analytical framework in several areas:

- Risk Management Strategy
- Awareness and Training
- Communication
- Information Protection Processes and Procedures

4) Partners — Without the cooperation of key business partners' security measures may be difficult to administer even within the most disciplined organizations. Broadcast organizations rely on network providers, satellite providers, equipment providers and service providers to ensure all security measures are in place. Unfortunately much of the legacy broadcast equipment still in use does not support security patching, auto updating or system monitoring through configuration management databases (CMDB) and other controls. It is recommended that broadcast organizations address this by making security an integral part of the requirements for purchasing new equipment and services. This is defined in the analytical framework in the following areas:

- Asset Management
- Risk Management
- Continuous Monitoring
- Detection Processes

Regarding hubbed operations, the obvious security and redundancy issues regarding protection of the feed from the hub require that two diverse routes should be employed with firewalls and VPN protection. All other data circuits, computers, digital streaming feeds, feeds



The Communications Security, Reliability and Interoperability Council IV
Final Report
Working Group 4
March 2015

NIST Sub-Category	Small Radio Station	TV Broadcast Station	Station Hub	Network Facility
ID.AM-1: Physical devices and systems within the organization are inventoried	Critical	Critical	Critical	Critical
ID.AM-2: Software platforms and applications within the organization are inventoried	Critical	Critical	Critical	Critical
ID.AM-3: Organizational communication and data flows are mapped		May Not be Critical	Critical	Critical
ID.AM-4: External information systems are catalogued			Critical	Critical
ID.AM-5: Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value	Critical	Critical	Critical	Critical
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Critical	Critical	Critical	Critical
ID.BE-1: Organization's role in the supply chain is identified and communicated			May be Critical	May be Critical
ID.BE-2: Organization's place in critical infrastructure and its industry sector is identified and communicated			May be Critical	May be Critical
ID.BE-3: Priorities for organizational mission, objectives and actives are established and communicated		May be Critical	Critical	Critical

47

The report discussed in the article includes a "matrix" based on the NIST framework as it applies to segments of the broadcast industry including small radio stations, local broadcast stations, station hub operations and broadcast networks. This is just a sample.

of any type should be protected as they would be in any other modern broadcast facility (see stations above). The best way to accomplish is to work closely with your vendor and security experts. It may be better if they are not the same company so there are proper checks and balances.

Also ensure everyone involved understands their roles and responsibilities. Make sure incidents and changes are properly logged and documented. There should always be a back out plan for major changes that have an adverse effect. Many systems should have a test lab to try new software and hardware before it is deployed, but this may not be possible in a large scale network that cannot be replicated. Put together a response plan and track recovery time for continuous improvement.

While a hubbed infrastructure provides efficiencies in a multi-station operation it is important to recognize that there is an increased risk which may impact the ability to provide essential and important services to listeners and viewers in multiple markets.

B. Broadcast Networks — Broadcast Firewall

As a Network Broadcaster Engineering Manager you have an obligation to the stations that depend on your distribution of content, including content for public interest and emergency information. There are many legacy broadcast systems that are not protected from cybersecurity attacks, monitored for threats nor properly controlled. Many IT groups have the necessary talent within their security staff to help identify the risks and create a plan to help mitigate them. It is important to gain support from your leadership including Technology Officer, Administrative, Programming and Finance before you review and then use the NIST Cybersecurity Framework to protect core network and critical infrastructure used in Broadcast Operations. The areas that should be focused on are access points to our critical production, ingest and broadcast systems. This involves possibly installing inbound/outbound firewall at all campuses. This broadcast demilitarized zone (DMZ) separates the broadcast Local Area Network (LAN) from the administration LAN, and provides the necessary protection. As a group, you should review the categories within the NIST Framework, and based upon your initial risk assessment focus on what has the greatest urgency to implement within your broadcast network**.** Then devise a plan for a review and recommendation on the following categories: (1) identify, (2) detect, (3) protect, (4) respond, and (5) recover.

Once you complete your analysis the next step is implementation. This is not as easy as one would imagine since many of the systems involved may never have had a firewall or constraints (such as virus protection, etc.), so the approach is to proceed cautiously and carefully:

1. *Access Control* — New Firewalls may need to be installed without restrictions so a full audit and analysis could be completed before making changes.
2. *Data Security* — A strict change management process should be instituted so any new Firewall rules could be quickly backed out if needed.
3. *Information Protection & Process Improvement* — A communication plan should be devised to ensure all stakeholders were informed of the risks.
4. *Anomalies & Events* — The network should be continuously monitored to detect potential cybersecurity events.

As you can see it is not only important to place cybersecurity controls within the network, but to collaborate within groups go ensure success. It is also recommended to have regular meetings with your new "cybersecurity committee" and meet regularly to discuss the latest threats, changes to our security protocols, and next step for implementing the framework. Each quarter you should review the NIST Framework against your business and look for new ways to improve our systems and processes. ■

RADIOWORLD

Email: radioworld@nbmedia.com
Website: www.radioworld.com
Telephone: (703) 852-4600
Business Fax: (703) 852-4582

EDITORIAL STAFF
EDITOR IN CHIEF, U.S. Paul J. McLane
EBOOK CONTRIBUTER Tom Vernon
GEAR & TECHNOLOGY EDITOR Brett Moss
INTERNATIONAL EDITOR IN CHIEF Marguerite Clark
TECHNICAL EDITOR, RWEE W.C. "Cris" Alexander
TECHNICAL ADVISOR Tom McGinley
CONTRIBUTING EDITOR Emily Reigart

ADMINISTRATION & PRODUCTION
PUBLISHER John Casey
EDITORIAL DIRECTOR Paul J. McLane
PRODUCTION MANAGERS Karen Lee & Lisa McIntosh
ADVERTISING COORDINATOR Caroline Freeland

Radio World Founded by Stevan B. Dana

ADVERTISING SALES REPRESENTATIVES
US REGIONAL & CANADA: John Casey
jcasey@nbmedia.com
T: 212-378-0400, ext. 512 | F: 330-247-1288

US REGIONAL: Michele Inderrieden
minderrieden@nbmedia.com
T: 212-378-0400, ext. 523 | F: 866-572-6156

EUROPE, MIDDLE EAST & AFRICA: Raffaella Calabrese
rcalabrese@nbmedia.com
T: +39-320-891-1938 | F: +39-02-700-436-999

LATIN AMERICA: Susana Saibene
susana.saibene@gmail.com
T: +34-607-31-40-71